



#5
PATENT

Attorney Docket No.: 16869P011500
Client Ref. No. 349901489US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Miyazaki Kunihiko et al.

Application No.: 09/693,713

Filed: October 19, 2000

For: DIGITAL SIGNING METHOD

Examiner: Not Assigned

Art Unit: 2131

RECEIVED

JUL 12 2001

Group 2100


**SUBMISSION OF PRIORITY
DOCUMENT**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Applicant respectfully submits priority document Japan P2000-081712 filed
March 17, 2000, to be made of record in the above-referenced application.

Respectfully submitted,


Kim Kanzaki, Ph.D.
Reg. No. 37,652

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel.: (650) 326-2400
Fax: (650) 326-2422
kk:amc
PA 3154251 v1

349901489US1



日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 3月17日

出 願 番 号

Application Number:

特願2000-081712

出 願 人

Applicant(s):

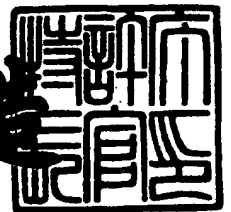
株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年11月 6日

特 許 庁 長 官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3090505

【書類名】 特許願

【整理番号】 K00005451

【提出日】 平成12年 3月17日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/00

【請求項の数】 20

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内

【氏名】 宮崎 邦彦

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内

【氏名】 佐々木 良一

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内

【氏名】 宝木 和夫

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内

【氏名】 洲崎 誠一

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内

【氏名】 森津 俊之

【発明者】

【住所又は居所】 神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所 情報システム事業部内

【氏名】 酒井 瑞洋

【発明者】

【住所又は居所】 東京都練馬区中村 2 - 1 4 - 1 7

【氏名】 岩村 充

【発明者】

【住所又は居所】 神奈川県横浜市青葉区柿の木台 1 3 - 4 5

【氏名】 松本 勉

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【先の出願に基づく優先権主張】

【出願番号】 平成11年特許願第301216号

【出願日】 平成11年10月22日

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9902691

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタル署名方法および装置

【特許請求の範囲】

【請求項 1】

メッセージに対するデジタル署名を検証するデジタル署名方法であって、
デジタル署名生成者側の装置において、

メッセージあるいはそのハッシュ値に、デジタル署名生成者が所有する秘密
鍵を作用させ、当該メッセージに対するデジタル署名を生成する署名生成ステ
ップと、

生成したデジタル署名とメッセージを含むデジタル署名付きメッセージを
配布するとともに、当該デジタル署名付きメッセージのログデータをログリス
トに登録する登録ステップと、を有し、

デジタル署名検証者側の装置において、

配布されたデジタル署名付きメッセージを、検証対象デジタル署名付きメ
ッセージとして受け付ける検証対象受付ステップと、

前記検証対象デジタル署名付きメッセージを配布したデジタル署名者のロ
グリストを取得する履歴取得ステップと、

前記検証対象デジタル署名付きメッセージのログデータが、前記ログリスト
に登録されているか否かを調べ、登録されている場合は、当該検証対象ディ
ジタル署名付きメッセージが前記デジタル署名生成者により配布されたものであ
ることを認証する第 1 の検証ステップと、を有すること

を特徴とするデジタル署名方法。

【請求項 2】

請求項 1 記載のデジタル署名方法であって、

前記登録ステップは、デジタル署名付きメッセージのログデータを、前記デ
ジタル署名者側の装置とは別に設けられた履歴管理センタが管理するログリス
トに登録すること

を特徴とするデジタル署名方法。

【請求項 3】

請求項 1 または 2 記載のデジタル署名方法であって、

前記デジタル署名検証者側の装置において、

前記第 1 の検証ステップに先立ち、前記検証対象デジタル署名付きメッセージに含まれるメッセージおよびデジタル署名と、前記秘密鍵と対の公開鍵とを用いて、前記検証対象デジタル署名付きメッセージに含まれるデジタル署名が当該検証対象デジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第 2 の検証ステップを、さらに有することを特徴とするデジタル署名方法。

【請求項 4】

請求項 1 または 2 記載のデジタル署名方法であって、

前記署名生成ステップは、メッセージあるいはそのハッシュ値と、前記ログリストに登録されている最新のログデータに含まれるデータ（前データ）とに、前記秘密鍵を作用させて、当該メッセージに対するデジタル署名を生成し、

前記登録ステップは、生成したデジタル署名と前データとメッセージを含むデジタル署名付きメッセージを配布するとともに、当該デジタル署名付きメッセージのログデータをログリストに登録すること

を特徴とするデジタル署名方法。

【請求項 5】

請求項 4 記載のデジタル署名方法であって、

デジタル署名検証者側の装置において、

前記第 1 の検証ステップに先立ち、前記検証対象デジタル署名付きメッセージに含まれるデジタル署名、前データおよびメッセージと、前記秘密鍵と対の公開鍵とを用いて、前記検証対象デジタル署名付きメッセージに含まれるデジタル署名が当該検証対象デジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第 2 の検証ステップを、さらに有すること を特徴とするデジタル署名方法。

【請求項 6】

請求項 4 または 5 記載のデジタル署名方法であって、

前記デジタル署名検証者側の装置において、

前記第 1 の検証ステップにより、前記検証対象デジタル署名付きメッセージが前記デジタル署名生成者により配布されたものであると認証された場合に、前記検証対象デジタル署名付きメッセージに含まれる前データが、前記ログリストにて前記検証対象デジタル署名付きメッセージのログデータより 1 つ前に登録されているログデータに含まれているか否かを調べ、含まれている場合は、前記ログリストが改ざんされていないことを認証する第 3 の検証ステップを、さらに有すること

を特徴とするデジタル署名方法。

【請求項 7】

請求項 4 または 5 記載のデジタル署名方法であって、

前記登録ステップは、デジタル署名付きメッセージのログデータを、配布先を付してログリストに登録し、

前記デジタル署名検証者側の装置において、

前記第 1 の検証ステップにより、検証対象デジタル署名付きメッセージが前記デジタル署名生成者により配布されたものであると認証された場合に、前記ログリストにて前記検証対象デジタル署名付きメッセージのログデータより 1 つ前に登録されているログデータに付された配布先から、デジタル署名付きメッセージを取得し、これが前記 1 つ前に登録されているログデータに含まれているか否かを調べ、含まれている場合は、前記ログリストが改ざんされていないことを認証する第 4 の検証ステップを、さらに有すること

を特徴とするデジタル署名方法。

【請求項 8】

請求項 2 記載のデジタル署名方法であって、

前記署名生成ステップは、メッセージあるいはそのハッシュ値と、前記ログリストに登録されている最新のログデータに含まれるデータ（前データ）とに、前記秘密鍵を作用させて、当該メッセージに対するデジタル署名を生成し、

前記登録ステップは、生成したデジタル署名と前データとメッセージを含むデジタル署名付きメッセージを配布するとともに、当該デジタル署名付きメ

ッセージのログデータを前記履歴管理センタが管理するログリストに登録し、かつ、

前記履歴管理センタにおいて、

前記登録ステップによるログデータのログリストへの登録に先立ち、前記検証対象デジタル署名付きメッセージに含まれる前データが、前記ログリストに登録されている最新のログデータに含まれている場合にのみ、当該ログデータの前記ログリストへの登録を許可する登録許可ステップを、さらに有すること

を特徴とするデジタル署名方法。

【請求項 9】

メッセージに対するデジタル署名を生成するデジタル署名装置であって、
メッセージあるいはそのハッシュ値に秘密鍵を作用させ、当該メッセージに対するデジタル署名を生成する署名生成手段と、

生成したデジタル署名とメッセージを含むデジタル署名付きメッセージのログデータを、記憶手段に格納されたログリストに登録する登録手段と、を有すること

を特徴とするデジタル署名装置。

【請求項 10】

請求項 9 記載のデジタル署名装置であって、

前記署名生成手段は、メッセージあるいはそのハッシュ値と、前記ログリストに登録されている最新のログデータに含まれるデータ（前データ）とに、前記秘密鍵を作用させ、当該メッセージに対するデジタル署名を生成し、

前記登録手段は、生成したデジタル署名とメッセージと前データを含むデジタル署名付きメッセージのログデータを、前記ログリストに登録すること

を特徴とするデジタル署名装置。

【請求項 11】

請求項 9 または 10 記載のデジタル署名装置であって、

当該デジタル署名装置は、電子計算機に接続可能に構成された、前記記憶手段を有する計算機能付き記憶媒体であること

を特徴とするデジタル署名装置。

【請求項 1 2】

請求項 1 1 記載のデジタル署名装置であって、

前記登録手段は、前記記憶手段に格納されたログリストに、新たに生成したデジタル署名付きメッセージのログデータを登録する場合、当該ログリストに登録されるログデータの数が所定数を超える場合は、当該ログリストに登録されているログデータのうち最も古いログデータを、前記電子計算機に出力して、前記電子計算機に用意されたログリストに登録するとともに、当該最も古いログデータを前記記憶手段から削除してから、新たに生成したデジタル署名付きメッセージのログデータを登録すること

を特徴とするデジタル署名装置。

【請求項 1 3】

請求項 9 記載のデジタル署名装置で生成されたデジタル署名を検証するデジタル署名検証装置であって、

検証すべきデジタル署名付きメッセージと前記デジタル署名装置の記憶手段に格納されているログリストを受け付ける入力手段と、

前記検証すべきデジタル署名付きメッセージのログデータが前記ログリストに登録されているか否かを調べ、登録されている場合は、当該検証すべきデジタル署名付きメッセージが、前記デジタル署名装置が関与して生成されたものであることを認証する第 1 の検証手段と、

前記検証すべきデジタル署名付きメッセージに含まれるデジタル署名およびメッセージと、前記デジタル署名装置が所持する秘密鍵と対の公開鍵とを用いて、前記検証すべきデジタル署名付きメッセージに含まれるデジタル署名が当該検証すべきデジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第 2 の検証手段と、を有すること

を特徴とするデジタル署名検証装置。

【請求項 1 4】

請求項 1 0 記載のデジタル署名装置で生成されたデジタル署名を検証するデジタル署名検証装置であって、

検証すべきデジタル署名付きメッセージと前記デジタル署名装置の記憶手

段に格納されているログリストを受け付ける入力手段と、

前記検証すべきデジタル署名付きメッセージのログデータが前記ログリストに登録されているか否かを調べ、登録されている場合は、当該検証すべきデジタル署名付きメッセージが、前記デジタル署名装置が関与して生成されたものであることを認証する第1の検証手段と、

前記検証すべきデジタル署名付きメッセージに含まれるデジタル署名、前データおよびメッセージと、前記デジタル署名装置が所持する秘密鍵と対の公開鍵とを用いて、前記検証すべきデジタル署名付きメッセージに含まれるデジタル署名が当該検証すべきデジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第2の検証手段と、

前記検証すべきデジタル署名付きメッセージに含まれる前データが、前記ログリストにて前記検証すべきデジタル署名付きメッセージのログデータより1つ前に登録されているログデータに含まれているか否かを調べ、含まれている場合は、前記ログリストが改ざんされていないことを認証する第3の検証手段と、を有すること

を特徴とするデジタル署名検証装置。

【請求項15】

請求項9記載のデジタル署名装置で生成されたデジタル署名を検証するためのプログラムが記憶された記憶媒体であって、

前記プログラムは、電子計算機に読取られ実行されることで、

検証すべきデジタル署名付きメッセージと前記デジタル署名装置の記憶手段に格納されているログリストを受け付ける入力手段と、

前記検証すべきデジタル署名付きメッセージのログデータが前記ログリストに登録されているか否かを調べ、登録されている場合は、当該検証対象デジタル署名付きメッセージが、前記デジタル署名装置が関与して生成されたものであることを認証する第1の検証手段とを、前記電子計算機上に構築すること

を特徴とする記憶媒体。

【請求項16】

メッセージに対するデジタル署名を検証するデジタル署名方法であって、

デジタル署名生成者側の装置において、

メッセージあるいはそのハッシュ値に、デジタル署名生成者が所有する秘密鍵を作用させてデジタル署名を生成する署名生成ステップと、

前記デジタル署名を信頼できる第3者であるタイムスタンプ発行局に送信し、その応答としてタイムスタンプを得るタイムスタンプ取得ステップと、

取得したタイムスタンプを前記メッセージに付し、デジタル署名付きメッセージとして配布する配布ステップと、を有し、

タイムスタンプ発行局側の装置において、

デジタル署名生成者から送られてきたデジタル署名と当該デジタル署名の受信時刻を含むデータに、タイムスタンプ発行局が所有する秘密鍵を作用させ、タイムスタンプを生成するタイムスタンプ生成ステップと、

前記タイムスタンプを前記デジタル署名生成者に送信する送信ステップと、を有し、

デジタル署名検証者側の装置において、

配布されたデジタル署名付きメッセージを、検証対象デジタル署名付きメッセージとして受け付ける検証対象受付ステップと、

前記検証対象デジタル署名付きメッセージに含まれるタイムスタンプに、タイムスタンプ発行局が所有する秘密鍵と対の公開鍵を作用させ、デジタル署名と時刻データを得る署名取得ステップと、

取得した時刻データが示す日時が、前記デジタル署名生成者より予め通知された期限を過ぎているか否かを調べ、過ぎていない場合は、取得したデジタル署名を有効と認証する第1の検証ステップと、を有すること

を特徴とするデジタル署名方法。

【請求項17】

請求項16記載のデジタル署名方法であって、

前記デジタル署名検証者側の装置において、

前記第1の検証ステップにより、デジタル署名が有効であると認証された場合に、当該デジタル署名と、前記検証対象デジタル署名付きメッセージに含まれるメッセージと、前記デジタル署名生成者の秘密鍵と対の公開鍵とを用い

て、前記デジタル署名が前記デジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第2の検証ステップを、さらに有すること を特徴とするデジタル署名方法。

【請求項18】

メッセージに対するデジタル署名を生成するデジタル署名システムであって、 デジタル署名装置とタイムスタンプ発行装置とを備え、

前記デジタル署名装置は、

メッセージあるいはそのハッシュ値に、自装置が所持する秘密鍵を作用させ、デジタル署名を生成する署名生成手段と、

前記デジタル署名を前記タイムスタンプ発行装置に送信し、その応答としてタイムスタンプを得るタイムスタンプ取得手段と、

取得したタイムスタンプを前記メッセージに付し、デジタル署名付きメッセージを作成する署名付きメッセージ作成手段と、を有し、

前記タイムスタンプ発行装置は、

前記デジタル署名生成装置から送られてきたデジタル署名と当該デジタル署名の受信時刻を含むデータに、自装置が所持する秘密鍵を作用させ、タイムスタンプを生成するタイムスタンプ生成手段と、

前記タイムスタンプを前記デジタル署名生成装置に送信する送信手段と、を有すること

を特徴とするデジタル署名システム。

【請求項19】

請求項18記載のデジタル署名システムで生成されデジタル署名を検証するデジタル署名検証装置であって、

検証すべきデジタル署名付きメッセージを受け付ける入力手段と、

前記検証すべきデジタル署名付きメッセージに含まれるタイムスタンプに、前記タイムスタンプ発行装置が所持する秘密鍵と対の公開鍵を作用させ、デジタル署名と時刻データを得る署名取得手段と、

前記署名取得手段で取得した時刻データが示す日時が、前記デジタル署名装置の使用者より予め通知された期限を過ぎているか否かを調べ、過ぎている場

合は、前記デジタル署名を有効と認証する第 1 の検証手段と、

前記デジタル署名と、前記検証すべきデジタル署名付きメッセージに含まれるメッセージと、前記デジタル署名生成装置が所持する秘密鍵と対の公開鍵とを用いて、前記デジタル署名が前記検証すべきデジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第 2 の検証手段と、を有すること

を特徴とするデジタル署名検証装置。

【請求項 2 0】

請求項 1 8 記載のデジタル署名システムで生成されデジタル署名を検証するためのプログラムが記憶された記憶媒体であって、

前記プログラムは、電子計算機に読取られ実行されることで、

検証すべきデジタル署名付きメッセージを受け付ける入力手段と、

前記検証すべきデジタル署名付きメッセージに含まれるタイムスタンプに、前記タイムスタンプ発行装置が所持する秘密鍵と対の公開鍵を作用させ、デジタル署名と時刻データを得る署名取得手段と、

前記署名取得手段で取得した時刻データが示す日時が、前記デジタル署名装置の使用者より予め通知された期限を過ぎているか否かを調べ、過ぎている場合は、前記デジタル署名を有効と認証する第 1 の検証手段と、

前記署名取得手段で取得したデジタル署名と、前記検証すべきデジタル署名付きメッセージに含まれるメッセージと、前記デジタル署名生成装置が所持する秘密鍵と対の公開鍵とを用いて、前記デジタル署名が前記検証すべきデジタル署名付きメッセージに含まれるメッセージに対してなされたものであるか否かを認証する第 2 の検証手段とを、前記電子計算機上に構築すること

を特徴とする記憶媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、デジタル署名技術に関する。

【0002】

【従来の技術】

電子的な文書などのデジタル化されたメッセージに、従来の印鑑に相当する機能を付与する技術であるデジタル署名が、電子商取引などにおけるネットワークの高度利用を可能にする技術として、注目されつつある。

【0003】

デジタル署名技術に関する文献としては、たとえば以下のものがある。

【0004】

文献1 : Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, "Handbook of Applied Cryptography" CRC Press, Inc. 1997

文献2 : Bruce Schneier, "Applied Cryptography Second Edition", John Wiley & Sons, Inc. 1996

文献3 : International Application Number PCT/US91/05386

文献4 : "Standard Specifications for Public Key Cryptography (Draft Version 11)" IEEE P1363, IEEE, July 1999

上記の各文献に記載のデジタル署名技術では、デジタル署名生成者は、署名対象となるメッセージMあるいはその特徴値、メッセージダイジェストであるハッシュ値に、自身が秘密裏に保持する秘密鍵を作用させることで、メッセージMに対するデジタル署名Aを生成する。そして、メッセージMにデジタル署名Aを付して公開する。デジタル署名検証者は、メッセージMに付されたデジタル署名Aを前記秘密鍵と対の公開鍵を作用させることで得た結果と、メッセージMあるいはそのハッシュ値とを比較する。両者が一致しない場合は、デジタル署名Aが生成された後にメッセージMに何らかの改ざんが加えられた可能性がある。このため、両者が一致する場合にのみ、デジタル署名AがメッセージMに対してなされたものであることを認証する。

【0005】

なお、上記の文献2のP75、"CHAPTER4 Intermediate Protocols, 4.1 TIMESTAMPING SERVICES"や文献3には、デジタル署名生成者が、自身が生成したメッセージに何らかの改ざんを加えて新たにデジタル署名を生成し、これらを元の

メッセージおよびデジタル署名と置き換えるような不正な行為を防止する技術が開示されている。該技術では、デジタル署名生成者は、署名対象となるメッセージ M_n あるいはそのハッシュ値と1つ前に生成したデジタル署名 A_{n-1} と時刻データを、自身が秘密裏に保持する秘密鍵を作用させることで、メッセージ M_n に対するデジタル署名 A_n を生成する。このようにすると、デジタル署名 A_n の次に生成されるデジタル署名 A_{n+1} には、1つ前に生成したデジタル署名 A_n が反映される。このため、デジタル署名生成者が自身が生成したメッセージ M_n に何らかの改ざんを加えて新たにデジタル署名 A_n を生成し、これらを元のメッセージ M_n およびデジタル署名 A_n と置き換えるような不正な行為を行うと、デジタル署名 A_{n+1} との間で整合がとれなくなる。

【0006】

【発明が解決しようとする課題】

ところで、上記のデジタル署名技術では、デジタル署名生成者が自身の秘密鍵を秘密裏に保持していることが前提となっている。すなわち、前記秘密鍵と対の公開鍵を用いて検証することができるデジタル署名を生成できるものは、前記秘密鍵を保持するデジタル署名生成者のみであることを前提としている。デジタル署名生成者の秘密鍵管理の不手際など何らかの理由により、第3者がデジタル署名生成者の秘密鍵を不正に入手し、デジタル署名生成者になりすましてデジタル署名を行った場合、上記のデジタル署名技術では、これを検知することができない。

【0007】

なお、International Application Number PCT/US93/1117には、メッセージと当該メッセージに対するデジタル署名に、デジタル署名生成者が保持する新たな秘密鍵を作用させることで、メッセージに対するデジタル署名を新たに生成する技術が開示されている。しかしながら、該技術は、近年の電子計算機の演算能力の飛躍的な向上や公開鍵から秘密鍵を求めるアルゴリズムの改良などにより、第3者がデジタル署名生成者の秘密鍵を不正に入手できる可能性が高まってきた場合に、以前に行ったデジタル署名のセキュリティを確保するための技術であり、秘密鍵を不正に入手した第3者がデジタル署名生成者になりすま

して行ったデジタル署名を検知することはできない。

【0008】

本発明は上記事情に鑑みてなされたものであり、本発明の目的は、デジタル署名生成者自身がしたデジタル署名と第3者がデジタル署名生成者になりすまして行ったデジタル署名とを識別可能なデジタル署名技術を提供することにある。

【0009】

【課題を解決するための手段】

上記目的を達成するために、本発明の第1の態様は、デジタル署名生成者側において、生成したデジタル署名とメッセージを含むデジタル署名付きメッセージの配布に先立ち、当該デジタル署名付きメッセージのログデータをログリストに登録する。ここで、ログデータとは、デジタル署名付きメッセージそのものであってもよいし、あるいは、デジタル署名付きメッセージに含まれるメッセージを当該メッセージのハッシュ値に置き換えたデジタル署名付きメッセージであってもよい。

本発明で用いられるハッシュ値とはハッシュ関数と呼ばれる、任意長の入力から固定長の値を出力するような関数によって計算される値を指す。安全性を確保する目的からは、同じ出力値を与えるような2つの異なる入力値を見出すことと出力がある与えられた値となる入力値を見出すこととが困難であるような関数を用いることが望ましい。ハッシュ関数のアルゴリズムはシステム全体に対して公開されているものとする。

【0010】

このようにすることで、デジタル署名検証者は、デジタル署名生成者からログリストを入手し、検証すべきデジタル署名付きメッセージのログデータが前記ログリストに登録されているか否かを調べることで、当該検証すべきデジタル署名付きメッセージが前記デジタル署名生成者により配布されたものであるか否かを検証することが可能となる。

【0011】

また、本発明の第2の態様は、デジタル署名生成者側において、自らが生成

したメッセージに対するデジタル署名を、信頼できる第3者であるタイムスタンプ発行局に送信し、タイムスタンプ発行局が秘密裏に保持する秘密鍵を用いて当該デジタル署名と時刻データを暗号化し、タイムスタンプを生成してもらう。そして、このタイムスタンプを前記メッセージに付して配布する。

【0012】

このようにすることで、デジタル署名検証者は、タイムスタンプ発行局の秘密鍵と対の公開鍵を用いて、メッセージに付されたタイムスタンプから時刻データとデジタル署名を取得し、この時刻データが示す日時が、デジタル署名生成者より予め通知された日時を過ぎているか否かを調べることで、デジタル署名が、デジタル署名生成者が有効と認めるものか否かを検証することが可能となる。

【0013】

【発明の実施の形態】

図1は本発明の第1実施形態が適用されたシステムの概略図である。

【0014】

図示するように、本システムは、デジタル署名付きメッセージを作成するデジタル署名者側装置 $1_1 \sim 1_n$ （以下、単にデジタル署名者側装置1とする）と、デジタル署名者側装置1が作成したデジタル署名付きメッセージを保持する購入者側装置 $3_1 \sim 3_n$ （以下、単に購入者側装置3とする）と、デジタル署名者側装置1が作成したデジタル署名付きメッセージの検証を行うデジタル署名検証者側装置5と、デジタル署名者側装置1が作成したメッセージのリストを公開し、購入者側装置3に代わってデジタル署名付きメッセージをデジタル署名者側装置1から入手する仲介者側装置7とを含んで構成される。

【0015】

なお、本発明の実施の形態において、メッセージとは、電子的な文書などのデジタルデータその他、イメージデータや音声データなどのデジタル化されたマルチメディアデータや、有価証券と同じ価値を持つデジタルデータなども含むものとする。また、本発明の実施の形態の説明にて用いられる文言「購入」とは、有償無償を問わず、デジタル署名者が作成したデジタル署名付きメッセ

ージを何らかの方法により入手する行為を指すものとする。

【0016】

図2は、デジタル署名者側装置1、購入者側装置3、デジタル署名検証者側装置5、仲介者側装置7、タイムスタンプ発行装置8の概略構成図である。

【0017】

各装置は、CPU11と、CPU11のワークエリアとして機能するRAM12と、ハードディスク装置などの外部記憶装置13と、CD-ROMやFDなどの可搬性を有する記憶媒体15からデータを読取る読取り装置14と、キーボードやマウスなどの入力装置16と、ディスプレイなどの表示装置17と、ネットワークを介して他の装置と通信を行うための通信装置18と、ICカード接続装置19と、上述した各構成要素間のデータ送受を司るインターフェース20を備えた、一般的な構成を有する電子計算機21に、計算機能付き記憶媒体であるICカード22を接続することで構築することができる。

【0018】

デジタル署名者側装置1の外部記憶装置13に格納されるのは、ICカード22に、メッセージに対するデジタル署名の生成を依頼し、メッセージにICカード22により生成されたデジタル署名を付して、デジタル署名付きメッセージとして配布するための署名付きメッセージ作成PG（プログラム）131と、自デジタル署名者側装置1が作成したデジタル署名付きメッセージの検証をデジタル署名検証者側装置5に依頼したり、デジタル署名検証者側装置5からの指示にしたがい、当該デジタル署名検証者側装置5がデジタル署名付きメッセージの検証を行うのに必要な情報を当該デジタル署名検証者側装置5に提供するための検証依頼PG（プログラム）132である。これらは、RAM12上にロードされ、CPU11により、署名付きメッセージ作成処理部111や検証依頼処理部112というプロセスとして具現化される。

【0019】

購入者側装置3の外部記憶装置13に格納されるのは、デジタル署名側装置1からデジタル署名付きメッセージを入手するための署名付きメッセージ入手PG（プログラム）331と、入手したデジタル署名付きメッセージの検証をディジタ

ル署名検証者側装置5に依頼するための検証依頼PG（プログラム）332である。これらは、RAM12上にロードされ、CPU11により署名付きメッセージ入手処理部311や検証依頼処理部312というプロセスとして具現化される。

【 0 0 2 0 】

デジタル署名検証者側装置5の外部記憶装置13に格納されるのは、デジタル署名者側装置1あるいは購入者側装置からの指示にしたがい、デジタル署名付きメッセージの検証を行う署名検証PG（プログラム）531である。これは、RAM12上にロードされ、CPU11により、署名検証処理部511というプロセスとして具現化される。

【 0 0 2 1 】

仲介者側装置7は、購入者側装置3に代わってデジタル署名付きメッセージをデジタル署名者側装置1から入手する。基本的に、図2と同様の構成を有する。購入者側装置3、デジタル署名検証者側装置5、仲介者側装置7には、ICカード接続装置はなくても良い。

【 0 0 2 2 】

これらのプログラムは、読取り装置14によりCD-ROMやFDなどの可搬性の記憶媒体15から読取られ、外部記憶装置13にインストールされるようにしてもよいし、あるいは、通信装置18を介してネットワークから外部記憶装置13にダウンロードされるようにしてもよい。

【 0 0 2 3 】

図3は、図2に示すICカード22の概略構成図である。

【 0 0 2 4 】

図示するように、ICカード22は、CPU221と、CPU221のワークエリアとして機能するRAM222と、各種プログラムやデータを記憶するEEPROM223と、ICカード接続装置19を介して電子計算機21と通信を行うI/O224とを有する。本発明において、EEPROMとは、データを電氣的に書き換え可能な不揮発性メモリを指す。

【 0 0 2 5 】

EEPROM223には、署名付きメッセージ作成処理部111からの指示にしたがい、メッセージに対するデジタル署名を生成するための署名生成PG（プログラム）22

31と、デジタル署名生成の際に用いる秘密鍵2232と、秘密鍵2232と対の公開鍵を含んだ公開鍵証明書2233と、デジタル署名生成の履歴を記録するための署名ログテーブル2234が格納されている。ここで、署名生成PG2231と秘密鍵2232は、ICカード22の発行時に設定され、ICカード22の外部からは読み出すことができないように設定されている。署名生成PG2231のように、カード発行時に書き込まれ、その後書き換えられることがないものは、EEPROM223ではなく書き換えできないROMに保存されていてもよい。公開鍵証明書2233は、ICカード22の発行時に設定され、ICカード22の外部からも読み出すことができるように設定されている。また、署名ログテーブル2234は、ICカード22の発行時には何ら記録されておらず、ICカード22がデジタル署名を生成する毎に、生成されたデジタル署名と当該署名対象メッセージのハッシュ値と当該署名対象メッセージの購入者名（購入者側装置3のアドレスなど）でなる署名ログ2235が追記される。この署名ログテーブル2234は、ICカード22の外部から読み出すことは可能であるが、ICカード22の外部から書き換えることができないように、またデータを消去することができないように、設定されているものとする。図3に示す例では、ICカード22でN回のデジタル署名生成処理が行われた後の状態を示しており、署名ログテーブル2234には、N個の署名ログ2235が記憶されている。

【 0 0 2 6 】

ICカード22の発行処理、すなわち、EEPROM223に、署名生成PG2231と秘密鍵2232と公開鍵証明書2233を格納・設定する処理は、ICカード発行業者が行うようにしてもよい。あるいは、ICカード発行業者は、EEPROM223に署名生成PG2231のみを格納した状態で発行し、ICカード22の所有者であるデジタル署名者が、秘密鍵2232と公開鍵証明書2233を、EEPROM223に格納・設定するようにしてもよい。

【 0 0 2 7 】

デジタル署名者が秘密鍵2232をEEPROM223に格納・設定する時は、ICカード発行業者によってあらかじめ秘密鍵生成プログラムをICカード22の内部に格納しておき、それをデジタル署名者が実行することにより、デジタル署名者自身も秘密鍵2232の値を知ることなく格納・設定するようにしたほうが望ましい。

【0028】

CPU221は、署名生成PG2231をRAM222上にロードして実行することで、署名生成処理部2211をプロセスとして具現化する。

【0029】

次に、図4を用いて、購入者側装置3がデジタル署名者側装置1からデジタル署名付きメッセージを入手する際の動作について説明する。

【0030】

デジタル署名者側装置1において、署名付きメッセージ作成処理部111は、購入者側装置3からメッセージの送信要求を受け取ると、その送信要求の対象であるメッセージを、たとえば各種メッセージが格納された外部記憶装置13から読み出し、これをハッシュ関数で評価することによりハッシュ値を求める。そして、メッセージのハッシュ値と送信要求を行った購入者側装置3のアドレスを署名生成処理部2211に送って署名生成を依頼する（S6101）。署名生成処理部2211は、送られてきたメッセージのハッシュ値に、秘密鍵2232を作用させ、メッセージに対するデジタル署名を生成する（S6102）。署名生成処理部2211は、メッセージのハッシュ値とデジタル署名と送信要求を行った購入者側装置3のアドレスからなる署名ログ2235を、署名ログテーブル2234に登録し（S6103）、デジタル署名と公開鍵証明書2233を、署名付きメッセージ作成処理部111に送る。署名ログテーブル2234はあらかじめインデックスをつけるなど、シーケンシャルにデータを管理できるようになっているほうが、各署名ログ間の時間的な前後関係がわかりやすくなるので好ましい。署名付きメッセージ作成処理部111は、送信要求の対象であるメッセージに該デジタル署名を付してデジタル署名付きメッセージを作成し、公開鍵証明書2233を添付して、送信要求を行った購入者側装置3に送信する（S6104）。

【0031】

購入者側装置3において、署名付きメッセージ入手処理部311は、入力装置36を介して購入者よりメッセージ入手要求が指示されると、当該メッセージを保持する入手先のデジタル署名者側装置1へメッセージ送信要求を送信し（S6001）、当該デジタル署名者側装置1からデジタル署名付きメッセージが送られてく

るのを待つ（S6002）。署名付きメッセージ入手処理部311は、受け取ったデジタル署名付きメッセージに含まれるデジタル署名の検証を行う。具体的には、当該デジタル署名に、当該デジタル署名付きメッセージに添付された公開鍵証明書2233の公開鍵を作用させるとともに、当該デジタル署名付きメッセージに含まれるメッセージからハッシュ値を求め、二つの結果を比較する（S6003）。両者が一致する場合（S6004でOKの場合）は、当該デジタル署名は、当該デジタル署名付きメッセージに含まれるメッセージに対してなされたものであると認証し、当該デジタル署名付きメッセージを受け入れ、入手先のデジタル署名者側装置1のアドレスを付して外部記憶装置33などに格納する（S6005）。両者が一致しない場合（S6004でNGの場合）は、認証せずに当該デジタル署名付きメッセージを破棄する（S6006）。

【 0 0 3 2 】

購入者装置は、実際に当該デジタル署名付きメッセージを受け入れる前に、必要に応じて、例えば当該デジタル署名付きメッセージの価値等に応じて、後述する署名検証依頼をデジタル署名検証者側装置5に依頼して署名を検証し、正当な署名であることを確認した後に受け入れるようにしてもよい。

【 0 0 3 3 】

仲介者側装置7が購入者側装置3を代行する場合は、図4に示す購入者側装置3のフローを仲介者側装置7が実行し、S6005で受け入れた署名付きメッセージを購入者側装置3に送信する。この場合、購入者側装置3は、S6003に示す検証処理を行わなくてすむので、購入者側装置3の負担を軽減できる。なお、仲介者側装置7は、各デジタル署名者側装置1が所有するメッセージに関する情報を予め入手し、各デジタル署名者側装置1が所有するメッセージのリストをWebなどを用いて各購入者側装置3に公開しておくことが好ましい。

【 0 0 3 4 】

デジタル署名者側装置1は、購入者側装置3からの依頼の有無にかかわらず、デジタル署名者の意思に基づいてデジタル署名付きメッセージを作成してもかまわない。この場合、図4に示す購入者側装置3のフローは行われなくなる。しかし、デジタル署名付きメッセージの購入者は、購入者側装置3を用

いて、後述する署名検証依頼をデジタル署名検証者側装置5に依頼することで、署名を検証することができる。

【 0 0 3 5 】

たとえば、メッセージが有価証券と同じ価値を持つデジタルデータ（ここでは、電子証券と呼ぶこととする）を例にとり説明すると、電子証券の発行者であるデジタル署名者は、デジタル署名者側装置1を用いて、図4に示すデジタル署名側装置1のフローを実行し、署名付き電子証券を作成・発行する。なお、電子証券の発行段階では、作成した署名付き電子証券の購入先が明らかでないので、署名ログテーブル2234に登録する署名ログ2235に購入先のアドレスは含まれない。

【 0 0 3 6 】

仲介者側装置7は、デジタル署名者側装置1が発行した署名付き電子証券を入手し、Webなどを用いて公開しておく。そして、購入者側装置3からの要求に応じて所望の署名付き電子証券を送信あるいは郵送等により送付する。電子証券の購入希望者は、実際に購入手続きを行う前に、購入者側装置3を用いて、購入予定の電子証券の検証をデジタル署名検証者側装置5に依頼し、有効性が確認された場合にだけ、実際の購入手続きを行うようにすることができる。

【 0 0 3 7 】

次に、図5を用いて、購入者側装置3がデジタル署名検証者側装置5に対して、デジタル署名者側装置1から入手したデジタル署名付きメッセージの検証を依頼する際の動作について説明する。

【 0 0 3 8 】

購入者側装置3において、検証依頼処理部312は、入力装置36を介して購入者より、自装置が保持しているデジタル署名付きメッセージの検証要求が指示されると、当該デジタル署名付きメッセージに当該デジタル署名付きメッセージの入手先であるデジタル署名者側装置1のアドレスを付して、デジタル署名検証者側装置5に送信し、検証を依頼する（S7001）。デジタル署名検証者側装置5から検証結果が送られてくるのを待ち（S7002）、検証結果をたとえば表示装置37に表示する（S7003）。

【 0 0 3 9 】

デジタル署名検証側装置5において、署名検証処理部511は、購入者側装置3からデジタル署名付きメッセージの検証要求を受信すると、当該要求とともに送られてきたデジタル署名付きメッセージに対し、ステップS6003、S6004と同様に、第1段階の検証を行う（S7101、S7102）。

【 0 0 4 0 】

S7102でOKの場合は、認証し、S7103に進む。S7102でNGの場合は、認証せず、検証結果を、検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（S7108）。

【 0 0 4 1 】

S7103では、署名検証処理部511は、デジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に、署名ログテーブル2234に記録された全ての署名ログ2235（署名ログリストと称する）の送信を要求し（S7103）、当該デジタル署名者側装置1から署名ログリストが送られてくるのを待ち（S7104）、署名検証処理部511は、デジタル署名付きメッセージに対し第2段階の検証を行う。具体的には、デジタル署名付きメッセージに含まれるデジタル署名とS7101で求めたメッセージのハッシュ値を含む署名ログが、入手した署名ログリスト中に登録されているか否かを調べる（S7105）。

【 0 0 4 2 】

登録されている場合（S7106でOKの場合）は、当該デジタル署名付きメッセージは、署名ログリストを提出したデジタル署名者側装置1で生成された正当なものであると認証し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（S7107）。

【 0 0 4 3 】

登録されていない場合（S7106でNGの場合）は、当該デジタル署名付きメッセージは、署名ログリストを提出したデジタル署名者側装置1で生成されていない、つまり、何らかの方法により秘密鍵2232を取得した第3者がデジタル署

名者になりすまして、不当に生成したものと判定し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（S7108）。

【 0 0 4 4 】

デジタル署名者側装置1において、検証依頼処理部112は、デジタル署名検証者側装置5から、署名ログリストの送信要求や検証結果が送られてくるのを待つ（S7201）。署名ログリストの送信要求が送られてきた場合は、EEPROM223の署名ログテーブル2234に登録されているすべての署名ログ2235を読み出して、デジタル署名検証者側装置5に送信する（S7202）。検証結果が送られてきた場合（S7203）は、その内容をたとえば表示装置17に表示する（S7204）。このように、デジタル署名者側装置1にも検証結果を伝えることで、たとえば、検証結果が、何らかの方法により秘密鍵2232を取得した第3者がデジタル署名者になりすまして不当にデジタル署名を生成していることを示している場合に、署名生成のための秘密鍵2232を変えるなどの対策を講じることが可能となる。

【 0 0 4 5 】

なお、本発明において、デジタル署名者側装置1からデジタル署名検証者側装置5への履歴ログリストの送付は、上記のように、ネットワークを用いて通信により行う他、たとえば郵送などのよりICカード22自体を送付することにより行うようにしてもよい。

【 0 0 4 6 】

次に、図6を用いて、デジタル署名者側装置1がデジタル署名検証者側装置5に対して、自デジタル署名者側装置1が生成したデジタル署名付きメッセージの検証を依頼する際の動作について説明する。

【 0 0 4 7 】

デジタル署名者側装置1において、検証依頼処理部112は、入力装置16を介してデジタル署名者より、デジタル署名付きメッセージの購入者である購入者側装置3のアドレスが入力され、当該デジタル署名付きメッセージの検証要求が指示されると、入力された購入者側装置3のアドレスをデジタル署名検証者側装置5に送信し、検証を依頼する（S8001）。その後、S8002に進み、図5に示

すフローのS7201～S7204の処理を実行する。

【0048】

デジタル署名検証側装置5において、署名検証処理部511は、デジタル署名者側装置1からデジタル署名付きメッセージの検証要求を受信すると、当該要求とともに送られてきたアドレスにより特定される購入者側装置3に対し、検証対象のデジタル署名付きメッセージの送信要求を、検証要求を送信したデジタル署名者側装置1のアドレスを付して行い（S8101）、当該メッセージが送られてくるのを待つ（S8102）。その後、S8103に進み、図5に示すフローのS7101～S7109の処理を実行する。

【0049】

購入者側装置3において、検証依頼処理部312は、デジタル署名検証者側装置5から検証対象のデジタル署名付きメッセージの送信要求が送られてくるのを待つ（S8201）。そして、当該要求に付されたアドレスにより特定されるデジタル署名者側装置1から入手したデジタル署名付きメッセージを、たとえば外部記憶装置33などから読み出して、デジタル署名検証者側装置5に送信する（S8202）。その後、S8203に進み、図5に示すフローのS7002～S7003の処理を実行する。

【0050】

本実施形態によれば、デジタル署名者側装置1は、自らが生成したデジタル署名とメッセージを含むデジタル署名付きメッセージの配布に先立ち、当該デジタル署名とメッセージのハッシュ値を含む署名ログ2235を署名ログテーブル2234に登録する。

【0051】

デジタル署名検証者側装置5は、デジタル署名生成者側装置1から登録された署名ログ2235からなる署名ログリストを入手し、検証すべきデジタル署名付きメッセージに含まれるメッセージのハッシュ値とデジタル署名を含む署名ログが登録されているか否かを調べる。このようにすることで、当該検証すべきデジタル署名付きメッセージがデジタル署名者側装置1により生成された正当なものであるか、それとも、何らかの方法により秘密鍵2232を取得した第3

者がデジタル署名者になりすまして不正に生成したものであるかを識別することが可能となる。

【 0 0 5 2 】

上記の実施形態とは異なり、EEPROM223に加えて、電子計算機21が備える外部記憶装置13にも署名ログテーブルを設定するようにしてもよい。そして、EEPROM223の署名ログテーブルに新たに生成した署名ログを登録することで、EEPROM223の署名ログテーブルに登録されるログ数が所定数（この数はEEPROM223の容量を考慮して設定すればよい）を超える場合は、EEPROM223の署名ログテーブルに登録されている最も古いログを外部記憶装置13の署名ログテーブルへ移動してから、前記新たな署名ログをEEPROM223の署名ログテーブルに登録するようにしてもよい。

【 0 0 5 3 】

あるいは、EEPROM223の署名ログテーブルに登録される署名ログを複数まとめて一度に外部記憶装置13の署名ログテーブルに登録するようにしてもよい。この外部記憶装置13の署名ログテーブルへの登録は、署名者の指示によって適宜行われるものとしてもよいし、所定数に達するたびに自動的に行われるようにしてもよい。

【 0 0 5 4 】

あるいは、新たに生成した署名ログを、EEPROM223の署名ログテーブルおよび電子計算機21の外部記憶装置13の署名ログテーブル各々に登録するとともに、前記新たに生成した署名ログをEEPROM223の署名ログテーブルに登録することで、EEPROM223の署名ログテーブルに登録されるログ数が所定数を超える場合は、EEPROM223の署名ログテーブルに登録されている署名ログのうち最も古いログをEEPROM223の署名ログテーブルから削除してから、前記新たに生成した署名ログをEEPROM223の署名ログテーブルに登録するようにしてもよい。

【 0 0 5 5 】

このようにすることで、EEPROM223の容量が小さい場合でも、デジタル署名者側装置1を実現することが可能となる。

【0056】

外部記憶装置13に設定される署名ログテーブルは、デジタル署名者が署名ログを改ざんするのを防ぐため、ICカード22からのみ書き込み可能に設定するか、または、CD-Rなどの書き換え不可の記憶媒体を用いることが好ましい。

【0057】

また、EEPROM223に署名ログテーブルを設定する代わりに、図1の構成に加えて、各デジタル署名者側装置1毎に署名ログテーブルを管理する、署名ログ管理装置9を新たに設けてもよい。そして、デジタル署名者側装置1は、新たにデジタル署名を生成する毎に、署名ログを、自デジタル署名者側装置1に対応付けられた署名ログテーブルに登録するようにしてもよいし、外部記憶装置13の署名ログテーブルへ登録する時と同様、複数の署名ログをまとめて、署名ログ管理装置9の自デジタル署名者側装置1に対応付けて設けられた署名ログテーブルに登録することにしてもよい。

【0058】

この場合、図5に示すフローのS7103において、デジタル署名検証者側装置5は、署名ログ管理装置9に対し、署名ログリストの送信要求を、検証対象デジタル署名付きメッセージを作成したデジタル署名者側装置1のアドレスを付して行う。また、図5に示すフローのS7201、S7202は署名ログ管理装置9が行う。署名ログ管理装置9は、署名ログリストの送信要求を受けた場合に、当該要求に付されたアドレスにより特定されるデジタル署名者側装置1の署名ログリストをデジタル署名検証者側装置5に送信する。このようにすることで、デジタル署名者による署名ログの改ざんを防止することができる。

【0059】

なお、署名ログ管理装置9は、デジタル署名検証者側装置5と同じ電子計算機上に構築してもかまわないし、同じ電子計算機と異なる電子計算機との両方に構築して、まず、署名ログを同じ計算機上の署名ログ管理装置によって管理し、一定数に達したらまとめて、異なる電子計算機上の署名ログ管理装置に登録することにしても構わない。

【0060】

プライバシーの問題などが無い場合には、署名ログ管理装置9内の署名ログデータを、署名が生成されてから一定の期間あるいは常に、ネットワークによって接続された他の装置に対し公開しておいてもよい。ただし、ログを書き換えたり消去したりすることのできないように設定しておくものとする。このようにすると、例えば、購入者は自分が関与する取引の記録が確かに署名者のログに反映していることを確認できるようになり、また、他の多くの装置から閲覧可能な状態で署名ログを管理しておくことにより、署名者自身による署名ログデータの改ざんが困難になるため、システム全体の信頼性を向上することができる。この署名ログを公開するための装置は、署名ログ管理装置とは別に設けてもよい。

【0061】

各ICカード毎に固有の情報を設定し、これを用いることにより登録された署名ログが確かにICカード22によって生成された署名に関するものであることを保証するようにしてもよい。例えば、ICカード発行業者がICカード発行時に、各ICカードに対し固有の情報を、各々のICカードの所有者となる署名者に対しても秘密裏に設定しておく。ICカードによって署名生成処理が行われる度に、そのICカードに固有の情報を、デジタル署名を生成するための秘密鍵2232とは異なる、MAC(Message Authentication Code)生成用の秘密鍵として利用して、当該デジタル署名に対するMACを生成し署名ログと共に署名ログテーブル中に登録しておき、デジタル署名検証者からの署名ログリストの送信要求に応じて、このMACを含んだ署名ログリストを送信する。

【0062】

上記方法により、署名ログの改ざんをより困難にできる。なぜなら、デジタル署名検証者はICカード発行業者から当該署名を生成したICカードの固有の情報を事前にあるいは必要に応じて入手し、それを用いてMACの正当性を確認することにより、署名ログの改ざんを検知できるからである。また署名者自身も知ることない情報を秘密鍵として利用しているため、署名者自身による署名ログの偽造も防ぐことができる。

【0063】

MACを署名ログテーブルに保管するだけでなく、購入者に対してデジタル署名付きメッセージと共に出力し、購入者が自分の購入したメッセージについている署名が正当なものであることの確認を補強する手段として利用できるようにしてもよい。

【0064】

署名ログ管理装置9を設けその中に署名ログテーブルを設定する場合には、署名ログ管理装置9もICカード発行業者から当該署名を生成したICカードの固有の情報を事前にあるいは必要に応じて入手できるようにし、署名ログを署名ログ管理装置9に設けられた署名ログテーブルに登録する時に、MACの正当性を検査し、正しいものだけを登録するようにしてもよい。この場合、さらに、MACの正当性を満たさない署名ログが登録されようとした時には、署名用の秘密鍵2232が暴露した等の理由で署名の偽造ができるようになったと見なし、署名者あるいはシステム全体に対し、警告を出し、以降その秘密鍵や署名方式を使わないようにしてもよい。

【0065】

各ICカード毎に固有の情報を、MAC生成用の秘密鍵として利用する代わりに、確かに特定のICカード22によって生成された署名であることを保証するための別のデジタル署名の秘密鍵として利用しても、MACの時と同様に、署名ログの偽造を困難にすることができる。上記方法では、ICカード22によって生成されたことを確認するための署名検証に各ICカード毎に固有の情報自体は必要なく、固有の情報に対応する誰もが入手可能な公開鍵情報があればよいことになるため、MACを使った時とは異なり、購入者が自分の購入したメッセージについている署名が正当なものであることの確認を補強する手段としては利用しやすい。

【0066】

上記方法では、解読アルゴリズムの改良による偽造の危険性を避けるという観点からは、購入者に署名付きメッセージとして送るデジタル署名とは異なるデジタル署名方式を利用したほうが望ましいし、ICカード22内の実装規模を小さくするという観点からは、同じデジタル署名方式を利用したほうが有利である

ので、状況に応じて選択すればよい。

【 0 0 6 7 】

各ICカード毎に固有の情報を動的に更新すれば、秘密鍵情報が固定されないことになるため、秘密鍵の解析がされにくくなるという利点がある。上記方法では、元となる各ICカード毎に固有の情報を使って正当性を確認するためには更新手段も知っている必要がある。例えば、固有の情報を利用する処理を行った後、固有の情報のハッシュ値を求め、それを新しい固有の情報として利用することにしてもよい。

【 0 0 6 8 】

次に、署名ログの改ざんをより効果的に防止できる第2実施形態について説明する。本実施形態におけるシステムの各装置の構成は、署名ログテーブル2234に格納される署名ログ2235の構成を除けば、基本的に第1実施形態のものと同様である。

【 0 0 6 9 】

購入者側装置3がデジタル署名者側装置1からデジタル署名付きメッセージを入手する際の動作は、図4に示す第1実施形態のものと同様であるが、デジタル署名者側装置1における署名生成の具体的な処理内容と、購入者装置3における署名検証の具体的な処理内容は異なる。

【 0 0 7 0 】

デジタル署名者側装置1において、署名生成処理部2211は、前回($N-1$ 回目)の署名生成処理により生成された署名ログ2235に含まれるメッセージ M_{N-1} のハッシュ値 $h(M_{N-1})$ とデジタル署名 $Sign_{N-1}$ との組 $(h(M_{N-1}), Sign_{N-1})$ (これを前データ P_{N-1} と称する)と、署名付きメッセージ作成処理部111から送られてきたメッセージ M_N のハッシュ値 $h(M_N)$ とに、秘密鍵2232を作用させ、デジタル署名 $Sign_N$ を生成する(S6102)。初めて(1回目)に署名を生成する時には、前データ P_0 としてあらかじめシステム全体に共通な値あるいは個々の装置に固有な値として決めておいた初期値IVを用いてもよいし、「なし」としてもよい。署名生成処理部2211は、前データ P_{N-1} とメッセージのハッシュ値 $h(M_N)$ とデジタル署名 $Sign_N$ と送信要求を行った購入者側装置3のアドレスからなる署名ログ2235を、署名ログテ

ーブル2234に登録する (S6103)。前データ P_{N-1} とデジタル署名 $Sign_N$ とEEPROM 223内に格納してある公開鍵証明書2233を、署名付きメッセージ作成処理部111に送る。署名付きメッセージ作成処理部111は、送信要求の対象であるメッセージ M_N に前データ P_{N-1} とデジタル署名 $Sign_N$ を付してデジタル署名付きメッセージを作成し、公開鍵証明書2233を添付して、購入者側装置3に送信する (S6104)。

【 0 0 7 1 】

上記の実施形態においては、デジタル署名 $Sign_N$ を生成する時に、前データ P_{N-1} ではなく、前データのハッシュ値 $h(P_{N-1})$ を用いてもよい。この場合、署名ログテーブルに格納するデータも前データ P_{N-1} のかわりに前データのハッシュ値 $h(P_{N-1})$ でよい。また、N回目の署名を行う時の前データとして、メッセージのハッシュ値 $h(M_{N-1})$ およびデジタル署名 $Sign_{N-1}$ に加え、N-1回目の署名を行う時に利用する前データ P_{N-2} のハッシュ値 $h(P_{N-1})$ の3つからなる組を用いるようにしてもよい。また、メッセージに対するハッシュ値を求めるのに利用するハッシュ関数と、前データに対するハッシュ値を求めるのに利用するハッシュ関数は、異なってもよい。なお、前データ P_{N-1} として $(h(M_{N-1}), Sign_{N-1})$ を使う場合のように、 P_i ($0 < i < N-1$) を保存しておかなくてもそれ以外のデータから計算により P_{N-1} を求められる場合には、データ保存領域削減のために前データを保存せず、必要に応じて計算によって求めることにしてもよい。

【 0 0 7 2 】

上記の処理により、署名ログテーブル2234に格納される署名ログ2235は、図7に示すように、前データとメッセージのハッシュ値とデジタル署名を含んで構成されるものとなる。

【 0 0 7 3 】

購入者側装置3において、S6003の比較ステップでは、当該デジタル署名付きメッセージに含まれるメッセージから求めたハッシュ値だけを比較対象とするのではなく、当該デジタル署名付きメッセージに含まれる前データとの組を比較対象とする。

【 0 0 7 4 】

次に、図 8 を用いて、購入者側装置 3 がデジタル署名検証者側装置 5 に対して、デジタル署名者側装置 1 から入手したデジタル署名付きメッセージの検証を依頼する際の動作について説明する。なお、以下では「偽造である」と判定されることが署名者にとって不利な結果であるような状況における検証動作を例に挙げて説明している。

【 0 0 7 5 】

図 8 において、S11001、S11002、S11003 の処理は、それぞれ、図 5 の S7001、S7002、S7003 と同じである。

【 0 0 7 6 】

検証依頼処理部 312 は、デジタル署名検証者側装置 5 から、デジタル署名付きメッセージを参考資料として送信する旨の要求が送られてくると（S11101）、当該要求に付されたアドレスにより特定されるデジタル署名者側装置 1 から入手したデジタル署名付きメッセージを、たとえば外部記憶装置 33 などから読み出して、デジタル署名検証者側装置 5 に送信する（S11102）。

【 0 0 7 7 】

デジタル署名検証側装置 5 において、署名検証処理部 511 は、当該デジタル署名付きメッセージに含まれるデジタル署名と、当該デジタル署名付きメッセージに添付された公開鍵証明書 2233 の公開鍵とを用いて、第 1 段階の検証を行う（S11201）。署名が認証された場合（S11202 で OK の場合の S11203、S11204 の処理）と認証されない場合（S11202 で NG の場合の S11214 の処理）は、それぞれ S7103、S7104、S7108 と同じである。

【 0 0 7 8 】

署名検証処理部 511 は、デジタル署名付きメッセージに対し第 2 段階の検証を行う。具体的には、デジタル署名付きメッセージに含まれるデジタル署名および前データと S11201 で求めたメッセージのハッシュ値とを含む署名ログが、入手した署名ログリストに登録されているか否かを調べる（S11205）。

【 0 0 7 9 】

登録されている場合（S11206 で OK の場合）は、S7106 と同じ判断を行い、ディ

ジタル署名付きメッセージに対し第3段階の検証を行う。具体的には、S11204で入手した署名ログリストにおいて、検証対象のデジタル署名付きメッセージに対応する署名ログよりも、1つ前に登録されている署名ログに含まれるメッセージのハッシュ値とデジタル署名を読み出す。たとえば、図7において、検証対象のデジタル署名付きメッセージに含まれるデジタル署名および前データとS11201で求めたメッセージのハッシュ値とを含む署名ログがN番目である場合、N-1番目の署名ログに含まれるメッセージのハッシュ値とデジタル署名を読み出す。署名検証処理部511は、1つ前に登録されている署名ログに含まれるメッセージのハッシュ値とデジタル署名を、検証対象のデジタル署名付きメッセージに含まれる前データと比較する。ここで、前データは、上述したように、1つ前に登録されている署名ログに含まれるメッセージのハッシュ値とデジタル署名で構成される（S11207）。

【 0 0 8 0 】

両者が一致しない場合（S11208でNGの場合）は、検証対象のデジタル署名付きメッセージに対応する署名ログが改ざんされたものと認定し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（S11216）。両者が一致する場合（S11206でOKの場合）は、S11209に進む。

【 0 0 8 1 】

S11209では、S11204で入手した署名ログリストにおいて、検証対象のデジタル署名付きメッセージに対応する署名ログよりも1つ前に登録されている署名ログに含まれる購入者のアドレスにより特定される購入者側装置3に対し、デジタル署名付きメッセージを参考資料として送信すべき旨の要求を、検証要求を送信したデジタル署名者側装置1のアドレスを付して行い、当該メッセージが送られてくるのを待つ（S11210）。

【 0 0 8 2 】

署名検証処理部511は、参考資料として入手したデジタル署名付きメッセージに対し第4段階の検証を行う。

【0083】

具体的には、S11210で入手したデジタル署名付きメッセージに含まれるメッセージのハッシュ値を求める。そして、S11210で入手したデジタル署名付きメッセージに含まれるデジタル署名および前データと当該メッセージのハッシュ値が、S11204で入手した署名ログリストにおいて、検証対象のデジタル署名付きメッセージに対応する署名ログよりも1つ前に登録されている署名ログの内容と一致するか否かを調べる（S11211）。

【0084】

両者が一致しない場合（S11212でNGの場合）は、検証対象のデジタル署名付きメッセージに対応する署名ログとこれより1つ前に記録されている参考資料のデジタル署名付きメッセージに対応する署名ログの両方が改ざんされ、その結果、S11208における第3段階の検証の結果がOKとされた可能性があると判断し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（S11217）。両者が一致する場合（S11212でOKの場合）は、検証対象のデジタル署名付きメッセージは、署名ログリストを提出したデジタル署名者側装置1で生成された正当なものであると認証し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（S11213）。デジタル署名者側装置1におけるステップS11301～S11305の処理は、ステップS7201～S7204と同じである。

【0085】

次に、図9を用いて、デジタル署名者側装置1がデジタル署名検証者側装置5に対して、自デジタル署名者側装置1が生成したデジタル署名付きメッセージの検証を依頼する際の動作について説明する。

【0086】

デジタル署名者側装置1において、ステップS12001では、S8001と同じ処理を行い、S12002では、図8に示すフローのS11301～S11305の処理を実行する。

【0087】

デジタル署名検証側装置5において、ステップS12101、S12102では、S8101、S

8102と同じ処理を行い、S12103では、図8に示すフローのS11201～S11217の処理を実行する。

【0088】

購入者側装置3において、ステップS12201、S12203では、S8201、S8202と同じ処理を行い、S12204では、図8に示すフローのS11002～S11003の処理を実行する。

【0089】

また、デジタル署名検証者側装置5から、参考資料としてのデジタル署名付きメッセージの送信要求が送られてくる場合（S12201でN0の場合のS12202の処理）は、検証依頼処理部312は、当該要求に付されたアドレスにより特定されるデジタル署名者側装置1から入手した参考資料としてのデジタル署名付きメッセージを読み出して、デジタル署名検証者側装置5に送信する（S12205）。

【0090】

本実施形態によれば、デジタル署名付きメッセージの正当性をより詳しく調べることが可能となる。

【0091】

上記の実施形態第3段階での署名検証において、検証対象のデジタル署名付きメッセージに対応する署名ログ、すなわちN番目の署名ログと、その一つ前のN-1番目の署名ログとの整合性（連鎖が正しく保たれているか否か）を調べたが、同様にしてN-1番目の署名ログとそのもう一つ前のN-2番目の署名ログとの整合性も調べるようにしてもよい。これを繰り返し署名ログリストに含まれるより多くの署名ログについて前後の連鎖が正しく保たれていることをチェックするように変更することにより、署名ログリストの信頼性の確認をより詳しく行うようにしてもよい。

【0092】

なお、上記の実施形態第3段階での署名検証において、署名ログテーブル2234に記録されている全ての署名ログのうち、検証対象のデジタル署名付きメッセージに対応する署名ログを含む任意数の組について、当該署名ログに含まれる前データが、1つ前の署名ログに含まれるデジタル署名およびメッセージのハッシュ値と一致するか否かを調べることで署名ログの改ざんを検出するようにして

もよい。

【0093】

当該デジタル署名付きメッセージのハッシュ値が、当該デジタル署名付きメッセージに対応する署名ログよりあとに登録されている一つ以上の署名ログに含まれるデジタル署名に反映されているか否かを調べることで、署名ログの改ざんを検出するようにしてもよい。

【0094】

本実施形態によれば、過去の電子署名を偽造するためには、偽造しようとする電子署名が作成される以前または以降の、一つ以上の電子署名を整合的に偽造しなければならなくなる。これは、過去の電子署名を偽造することの困難性を増加させることによって、署名を偽造することによる正しい業務実行者への攻撃を難しくするとともに、正しい業務実行者にとっては、自らをアリバイ偽造が困難な地位におくことによって、悪意による攻撃にさらされたときの調停者への証明力を高める効果をもたらす。

【0095】

上記実施形態では、第2段階での署名検証で、検証対象のデジタル署名付きメッセージに含まれる署名データが、署名者から提出された署名ログリストに含まれない場合には検証対象のデジタル署名は偽造されたものであると判定し、含まれた場合には第3段階、第4段階で署名ログリストの正当性を確認していた。これは「偽造である」と判定されることが署名ログリストを提出する署名者にとって不利な結果である場合、署名者が改ざんされた署名ログリストを提出することは考えにくいためである。

【0096】

反対に、「正当な署名である」と判定されることが署名ログリストを提出する署名者にとって不利な結果であるような場合には、第2段階での署名検証で、検証対象の署名データが、提出された署名ログリストに含まれていた場合に、正当なものであると判定し、含まれていなかった場合には、第3段階、第4段階で署名ログリストの正当性を確認するようにしてもよい。

【0097】

あるいは、S11204で署名ログリストを受信した後に、まず署名ログリストの正当性を確認し、その後、検証対象の署名データが、正当性が確認された署名ログリストにあれば、正当な署名であると判定するようにしてもよい。

【0098】

署名者が、データの破壊等何らかの理由で、署名ログリストの全体を検証者に提出することができなかった時には、一般的には、署名ログリスト(の一部)として提出されてきた情報の全てを信頼することはできないが、以下に示す方法に従えば、送られてきた情報のうち、信頼できる署名ログを抽出することができる。

【0099】

デジタル署名検証側装置5においては、提出されてきた署名ログリストに含まれる署名ログのうち、署名者自身が制御できない領域に対応する署名が存在する証拠があるものは信頼できる署名ログと見なすことができる。

例えば、EEPROM223領域に署名ログ2235として保存された署名は、ICカード22を使って署名者が署名生成をした時に、自動的に書き込まれる。この領域は書き換えや消去ができないように設定されているため、署名者自身によっても制御できない(改ざんできない)。したがって、EEPROM223領域に保存された署名に対応するログは信頼できると見なしてよい。

同様に、署名ログ管理装置9等の信頼できる第3者に保存されている署名も、署名者自身によっても制御できないため、この署名に対応する署名ログは信頼できると見なせる。

また、署名検証者による署名検証が行われるより以前のある時点、例えば署名者により生成された直後に、新聞・放送等により公開され、不特定多数によって知られていた署名も、その時点以降に署名者が当該署名が存在しなかったことにすることは非常に困難であり、署名者自身によっても制御できないため、この署名に対応する署名ログは信頼できると見なせる。

利害関係のない他の購入者などが署名を(例えば署名ログとして)所有している場合も同様に信頼できる署名ログと見なすことができる。

【0100】

さらに、これら信頼できる署名ログの一つ前の署名ログとの整合性、つまり、連鎖が正しく保たれていることが確認できれば、この一つ前の署名ログも信頼できる署名ログと見なすことができる。なぜなら本発明では、署名ログに、一つ前のメッセージあるいは署名などのハッシュ値が含まれているため、たとえ秘密鍵の暴露等によりデジタル署名そのものの偽造が容易になったとしても、信頼できる署名ログに含まれるハッシュ値と一致するように、一つ前の署名ログを偽造することは非常に困難であるからである。この手順を繰り返し適用することにより、信頼できる署名ログからはじめて、連鎖を保っていることを確認しながら、一つずつ前、すなわち、より以前になされた署名ログ方向に遡ることができた範囲の署名ログを、提出されてきた署名ログリストに含まれるうちの信頼できる部分と見なすことができる。

【0101】

本実施形態においても、上記の第1実施形態と同様に、EEPROM223に加えて、電子計算機21が備える外部記憶装置13にも署名ログテーブル2234を設定するようにしてもよい。

EEPROM223に署名ログテーブル2234を設定する代わりに、すでに説明したように、各デジタル署名者側装置1毎に署名ログテーブルを管理する署名ログ管理装置9を設けるようにしてもよい。

この署名ログ管理装置9は、上記の第1実施形態と同様、デジタル署名検証者側装置5と同じ電子計算機上に構築されるようにしてもよい。

上記第1実施形態と同様、ICカード毎に固有の情報(製造番号など)を用いて、確かにそのICカードによって署名生成が行われたということを保証するためのデータを生成することにしてもよい。

署名ログ管理装置9を設ける場合、署名ログの署名ログリストへの登録に先立って、署名ログ管理装置9にて、図8に示すフローのS11207、S11208(第3段階の署名検証)を行い、当該署名ログに含まれる前データが、署名ログリストに登録されている最新の署名ログデータに含まれているメッセージのハッシュ値およびデジタル署名と一致する場合にのみ、当該署名ログの署名ログリストへの登

録を許可するようにしてもよい。この場合、デジタル署名検証者側装置5にて、図8に示すフローのS11207、S11209（第3段階の署名検証）を省略することも可能である。

【0102】

上記第1実施形態と同様、複数の署名ログをまとめて署名ログ管理装置9の管理する署名ログリストへ登録することにしてもよい。この場合、さらに、署名ログリストへの登録を行った旨、メッセージを作成し、このメッセージに対し署名生成を行うようにして、自らの署名ログリスト内に、署名ログリストへの登録を行った事実を反映するようにしてもよい。

【0103】

次に、上記の第1実施形態において、デジタル署名に時刻情報を含めることで、当該時刻情報からもデジタル署名の有効・無効を判定できるようにした第3実施形態について説明する。

【0104】

本システムは、図1に示す第1実施形態のシステムに、デジタル署名者側装置1から送られてきたデジタル署名に対してタイムスタンプを発行するタイムスタンプ発行装置8が追加された構成となる。

【0105】

タイムスタンプ発行装置8の概略構成は、図2に示す構成と同様である。

【0106】

外部記憶装置13には、デジタル署名者側装置1から送られてきたデジタル署名および時刻データを暗号化してタイムスタンプを生成するためのタイムスタンプ発行PG（プログラム）831と、タイムスタンプ生成の際に用いる秘密鍵832と、秘密鍵832と対の公開鍵を含んだ公開鍵証明書833が格納されている。これらはRAM12上にロードされCPU11により、タイムスタンプ発行処理部811というプロセスとして具現化される。

【0107】

図10を用いて、購入者側装置3がデジタル署名者側装置1からデジタル署名付きメッセージを入手する際の動作について説明する。

【 0 1 0 8 】

デジタル署名者側装置1において、図4に示すS6101～S6103の処理を実行する（S15101）。署名付きメッセージ作成処理部111は、署名生成処理部2211から送られてきたデジタル署名を、タイムスタンプ発行装置8に送信して、タイムスタンプの発行を依頼する（S15102）。署名付きメッセージ作成処理部111は、タイムスタンプ発行装置8からタイムスタンプを受け取ると（S15103）、送信要求の対象であるメッセージに当該タイムスタンプを付してデジタル署名付きメッセージを作成し、これに、署名生成処理部2211からデジタル署名とともに送られてきた公開鍵証明書2233と、タイムスタンプ発行装置8からタイムスタンプとともに送られてきた公開鍵証明書833を添付して、送信要求を行った購入者側装置3に送信する（S15104）。

【 0 1 0 9 】

タイムスタンプ発行装置8において、タイムスタンプ発行処理部811は、デジタル署名者側装置1からデジタル署名が送られてくると、タイムスタンプを生成する（S15201）。具体的には、デジタル署名者側装置1から送られてきたデジタル署名と当該デジタル署名の受信時刻を示す時刻データを、外部記憶装置83に格納してある秘密鍵832を用いて暗号化することで、タイムスタンプを生成する。タイムスタンプ発行処理部811は、生成したタイムスタンプに、外部記憶装置83に格納してある公開鍵証明書833を付して、デジタル署名を送信したデジタル署名者側装置1に送信する（S15202）。

【 0 1 1 0 】

購入者側装置3において、図4に示すS6001～S6002の処理を実行し、デジタル署名付きメッセージを取得する（S15001）。次に、署名付きメッセージ入手処理部311は、受け取ったデジタル署名付きメッセージに含まれるタイムスタンプを、当該メッセージに添付された公開鍵証明書821の公開鍵（タイムスタンプ発行装置8の公開鍵）を用いて復号化することで、デジタル署名を得る（S15002）。S6004～S6006の処理を実行して、デジタル署名の検証を行う（S15003）。

【 0 1 1 1 】

図 1 1 を用いて、購入者側装置 3 がデジタル署名検証者側装置 5 に対して、デジタル署名者側装置 1 から入手したデジタル署名付きメッセージの検証を依頼する際の動作について説明する。

【 0 1 1 2 】

なお、本実施形態において、デジタル署名者側装置 1 の使用者であるデジタル署名者は、自身が秘密裏に保持する秘密鍵 2232 が暴露され、第 3 者が不正に入手した可能性がある場合、暴露の日時を指定して速やかにデジタル署名検証者に連絡するものとする。そして、デジタル署名検証者は、デジタル署名者が通知した日時と当該デジタル署名者が使用するデジタル署名者側装置 1 のアドレスとを対応付けて、デジタル署名検証者側装置 5 の外部記憶装置 53 に格納させることとする。

【 0 1 1 3 】

検証依頼処理部 312 は、図 5 に示すフローの S7001 ～ S7003 の処理を実行し、デジタル署名検証者側装置 5 から検証結果を入手する (S16001)。

【 0 1 1 4 】

デジタル署名検証側装置 5 において、署名検証処理部 511 は、購入者側装置 3 からデジタル署名付きメッセージの検証要求を受信すると、当該要求とともに送られてきたデジタル署名付きメッセージに含まれるタイムスタンプを、当該デジタル署名付きメッセージに添付された公開鍵証明書 821 の公開鍵 (タイムスタンプ発行装置 8 の公開鍵) を用いて復号化することで、時刻データとデジタル署名を得る (S16101)。

【 0 1 1 5 】

署名検証処理部 511 は、外部記憶装置 53 を調べて、デジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置 1 に対して、秘密鍵 2232 の暴露日時が設定されているか否かを確認する (S16102)。暴露日時が設定されている場合は、S16103 に進み、設定されていない場合は、S16105 に進んで、図 5 に示す S7101 ～ S7109 の処理を実行する。

【 0 1 1 6 】

S16103では、署名検証処理部511は、S16101で得た時刻データが示す日時が外部記憶装置53に設定されている暴露時刻より新しいか否かを調べる（S16103）。新しい場合は、検証対象のデジタル署名付きメッセージは無効であると判定し、その結果を検証要求を送信した購入者側装置3とデジタル署名付きメッセージに付されたアドレスにより特定されるデジタル署名者側装置1に送信する（S16104）。新しくない場合は、S16105に進んで、図5に示すS7101～S7109の処理を実行する。

【 0 1 1 7 】

デジタル署名者側装置1において、検証依頼処理部112は、図5に示すS7201～S7204の処理を実行する（S16201）。

【 0 1 1 8 】

次に、図12を用いて、デジタル署名者側装置1がデジタル署名検証者側装置5に対して、自デジタル署名者側装置1が生成したデジタル署名付きメッセージの検証を依頼する際の動作について説明する。

【 0 1 1 9 】

デジタル署名者側装置1の処理は、図6に示すS8001～S8002の処理と同じである。

【 0 1 2 0 】

デジタル署名検証側装置5において、署名検証処理部511は、デジタル署名者側装置1からデジタル署名付きメッセージの検証要求を受信すると、当該要求とともに送られてきたアドレスにより特定される購入者側装置3に対し、検証要求を送信したデジタル署名者側装置1のアドレスを付したデジタル署名付きメッセージの送信を要求し、当該メッセージが送られてくるのを待つ。その後、図11に示すS16101～S16105の処理を実行する（S17103）。

【 0 1 2 1 】

購入者側装置3の処理は、図6に示すS8201～S8203の処理と同じである。

【 0 1 2 2 】

本実施形態によれば、デジタル署名検証者側装置3は、タイムスタンプ発行

局側装置8の公開鍵を用いて、検証対象のデジタル署名付きメッセージに含まれるタイムスタンプを復号化してデジタル署名と時刻データを取得する。この時刻データが示す日時が、デジタル署名生成者より通知された暴露日時を過ぎているか否かを調べることで、デジタル署名の検証に先立ち、当該デジタル署名の有効・無効を調べることができる。

【0123】

上記の実施形態において、デジタル署名者側装置1は、タイムスタンプの発行依頼を、間欠的（たとえば、 m 回に1回）に行うようにしてもよい。タイムスタンプが付与されていないデジタル署名付きメッセージに対して、デジタル署名生成者より通知された暴露日時に基づいたデジタル署名の有効・無効を判定する場合には、以下のようにして行えばよい。

【0124】

デジタル署名者側装置1は、デジタル署名をタイムスタンプ発行装置8に送信してタイムスタンプの発行を依頼した場合、図12に示すように、タイムスタンプ発行装置8から送られてきたタイムスタンプを、当該スタンプの対象となるデジタル署名の署名ログ2235に含めて署名ログテーブル2234に登録する。なお、署名ログテーブル2234への登録は時系列的に行う。

【0125】

デジタル署名検証者側装置3は、署名ログテーブル2234において、検証対象のデジタル署名付きメッセージに対応する署名ログより前に登録されている署名ログであって、タイムスタンプが記録されている署名ログを検出し、当該タイムスタンプを復号化して時刻データを得る。署名ログテーブル2234への登録は、時系列的に行われているので、検証対象のデジタル署名付きメッセージは、少なくとも復号化された時刻データが示す日時より後に生成されたものである。したがって、デジタル署名者から通知された暴露日時がこの復号化された時刻データが示す日時より前である場合には、検証対象のデジタル署名付きメッセージは無効と判定する。

【0126】

さらに、第2実施形態において、タイムスタンプによるデジタル署名の有効

・無効を判定できるようすることも可能である。第1実施形態や第2実施形態と組み合わせることなく、タイムスタンプによるデジタル署名の有効・無効を判定できるようにすることも可能である。

【0127】

上記の各実施形態とは異なり、署名ログテーブル2234を格納する記憶装置の容量に余裕がある場合などに、メッセージをそのものを署名ログ2235に含めるようにしてもよい。

【0128】

上記の各実施形態とは異なり、デジタル署名者側装置1で行うべき全ての処理を電子計算機21内で行うようにしてもよい。

【0129】

本発明には、上記の各実施形態とは異なり、デジタル署名と、メッセージ（第2実施形態ではこれに加えて前データ）と、デジタル署名者が所有する秘密鍵と対の公開鍵を用いて、前記デジタル署名が前記メッセージに対してなされたものであるか否かを認証することが可能な、様々な署名方法を適用できる。

【0130】

【発明の効果】

以上説明したように、本発明によれば、デジタル署名生成者自身がしたデジタル署名と第3者がデジタル署名生成者になりすまして行ったデジタル署名とを識別可能なデジタル署名技術を提供することができる。

【図面の簡単な説明】

【図1】

本発明の第1実施形態が適用されたシステムの概略図である。

【図2】

図1に示すデジタル署名者側装置1、購入者側装置3、デジタル署名検証者側装置5、仲介者側装置7、タイムスタンプ発行装置8の概略構成図である。

【図3】

図2に示すICカード22の概略構成図である。

【図 4】

本発明の第 1 実施形態において、購入者側装置 3 がデジタル署名者側装置 1 からデジタル署名付きメッセージを入手する際の動作を説明するためのフロー図である。

【図 5】

本発明の第 1 実施形態において、購入者側装置 3 がデジタル署名検証者側装置 5 に対して、デジタル署名者側装置 1 から入手したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【図 6】

本発明の第 1 実施形態において、デジタル署名者側装置 1 がデジタル署名検証者側装置 5 に対して、自デジタル署名者側装置 1 が生成したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【図 7】

本発明の第 2 実施形態において、署名ログテーブル 2234 に格納されるデータの構成を説明するための図である。

【図 8】

本発明の第 2 実施形態において、購入者側装置 3 がデジタル署名検証者側装置 5 に対して、デジタル署名者側装置 1 から入手したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【図 9】

本発明の第 2 実施形態において、デジタル署名者側装置 1 がデジタル署名検証者側装置 5 に対して、自デジタル署名者側装置 1 が生成したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【図 1 0】

本発明の第 3 実施形態において、購入者側装置 3 がデジタル署名者側装置 1 からデジタル署名付きメッセージを入手する際の動作を説明するためのフロー図である。

【図 1 1】

本発明の第 3 実施形態において、購入者側装置 3 がデジタル署名検証者側装

置5に対して、デジタル署名者側装置1から入手したデジタル署名付きメッセージの検証を依頼する際の動作を説明するためのフロー図である。

【図 1 2】

本発明の第 3 実施形態の変形例において、署名ログテーブル2234に格納されるデータの構成を説明するための図である。

【符号の説明】

- 1…デジタル署名者側装置
- 3…購入者側装置
- 5…デジタル署名検証者側装置
- 7…仲介者側装置
- 8…タイムスタンプ発行装置
- 9…署名ログ管理装置
- 11,31,51,81,221…CPU
- 12,32,52,82,222…RAM
- 13,33,53,83…外部記憶装置
- 14,34,54,84…読取り装置
- 15,35,55,85…記憶媒体
- 16,36,56,86…入力装置
- 17,37,57,87…表示装置
- 18,38,58,88…通信装置
- 19…ICカード接続装置
- 20,40,60,90…インターフェース
- 21,41,61,91…電子計算機
- 22…ICカード
- 111…署名付きメッセージ作成処理依頼部
- 112,312…検証依頼処理部
- 131…署名付きメッセージ作成プログラム
- 132,332…検証依頼プログラム
- 223…EEPROM

224… I/O

311… 署名付きメッセージ入手処理部

331… 署名付きメッセージ入手プログラム

511… 署名検証処理部

531… 署名検証プログラム

811… タイムスタンプ発行処理部

831… タイムスタンプ発行プログラム

832, 2232… 秘密鍵

833, 2233… 公開鍵証明書

2211… 署名生成処理部

2231… 署名生成プログラム

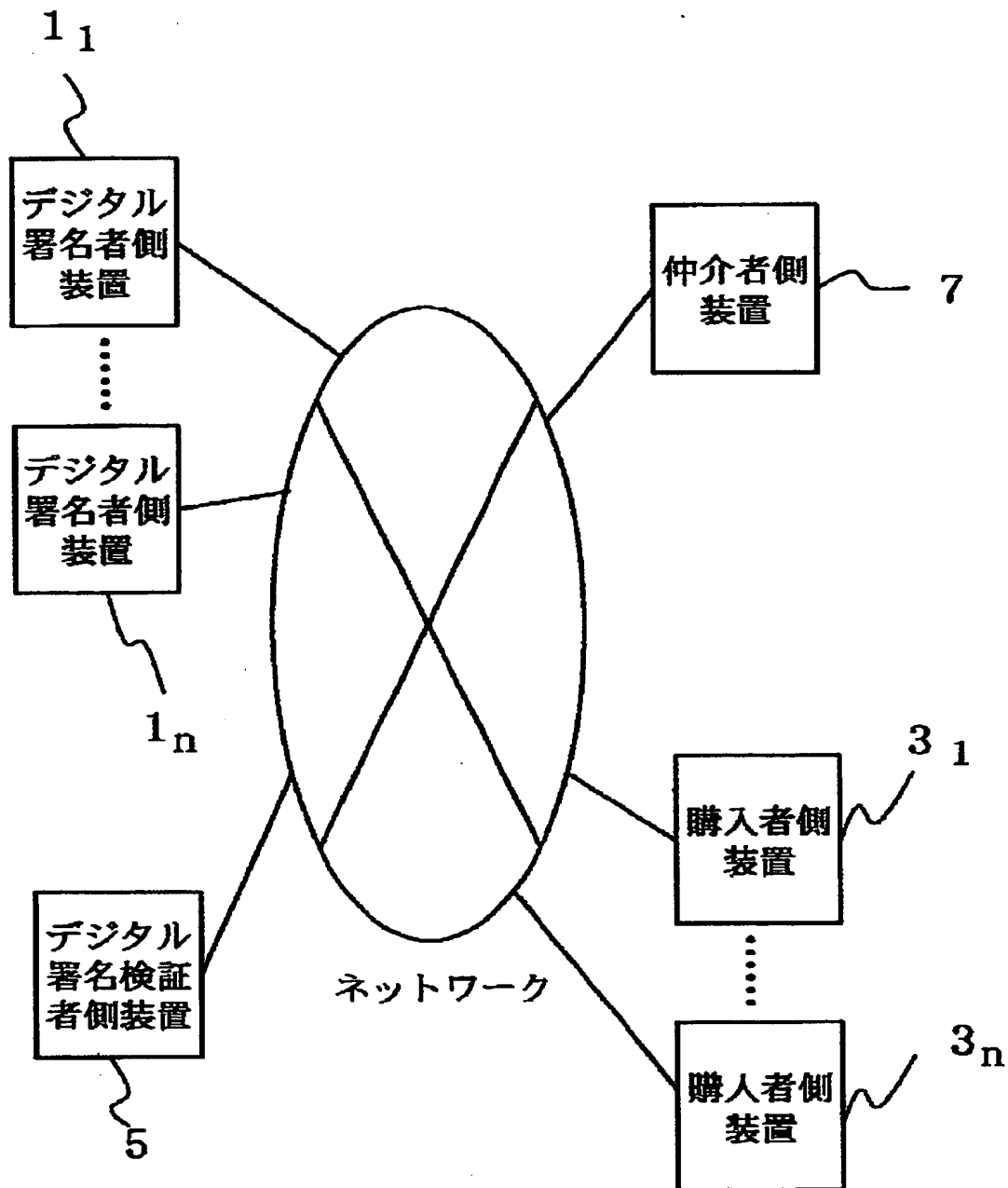
2234… 署名ログテーブル

2235… 署名ログ

【書類名】 図面

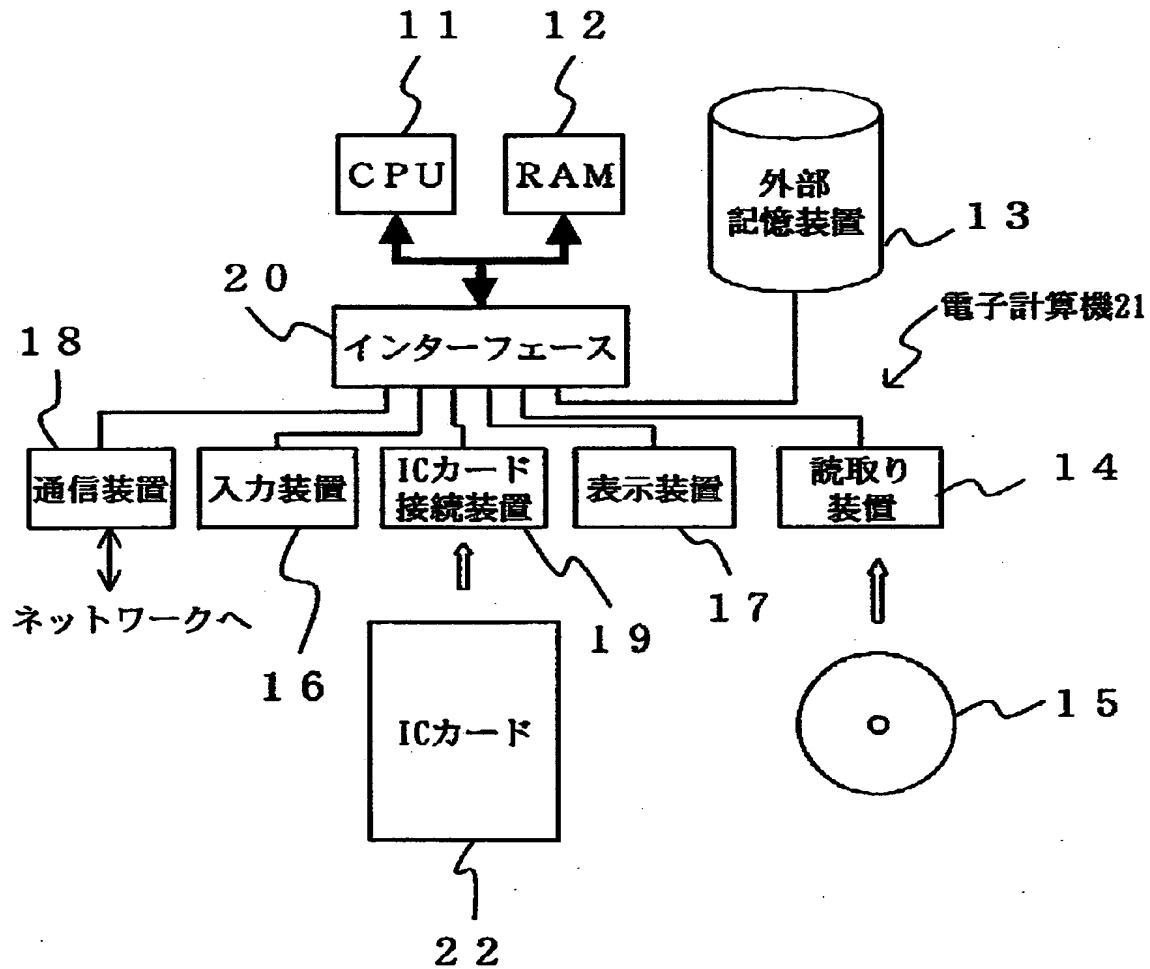
【図1】

図1



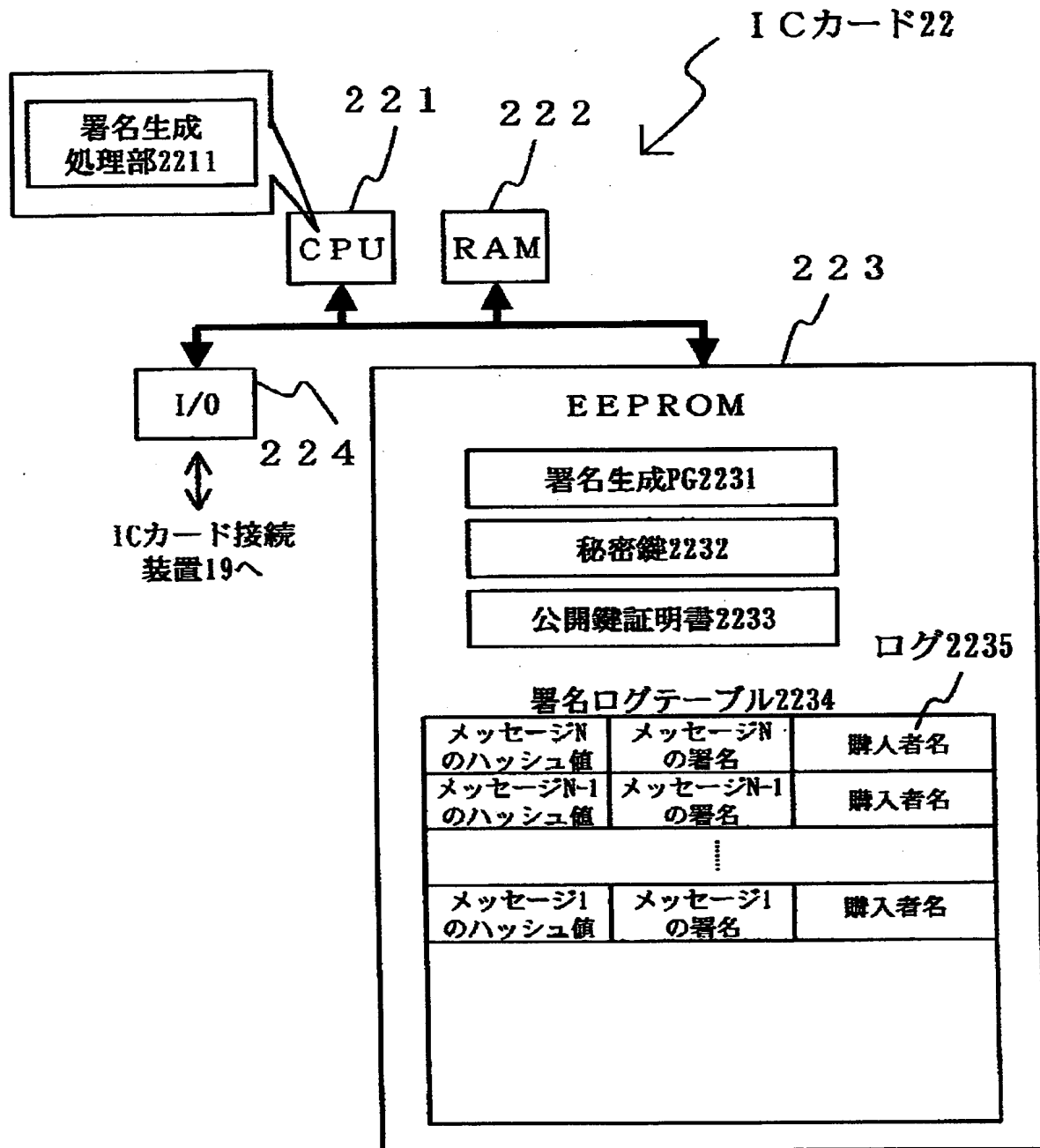
【図2】

図2



【図3】

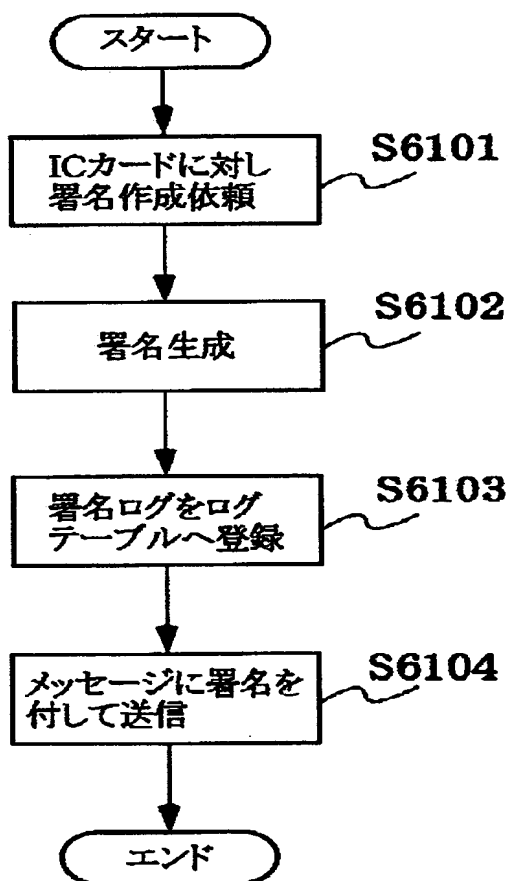
図3



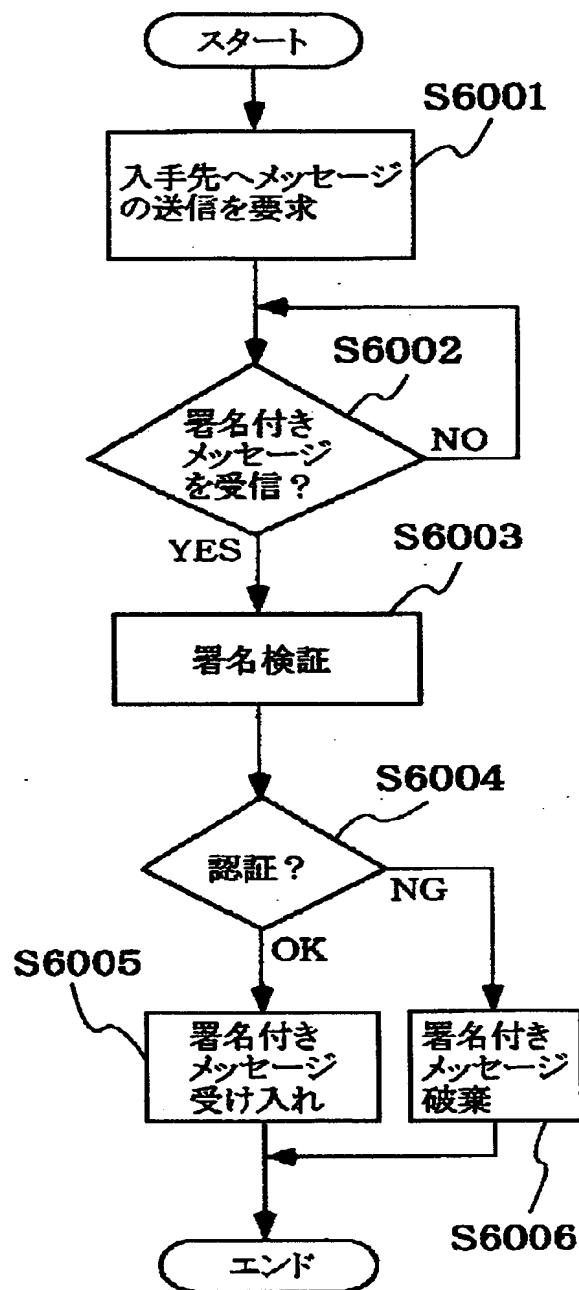
【図4】

図 4

デジタル署名者側装置1

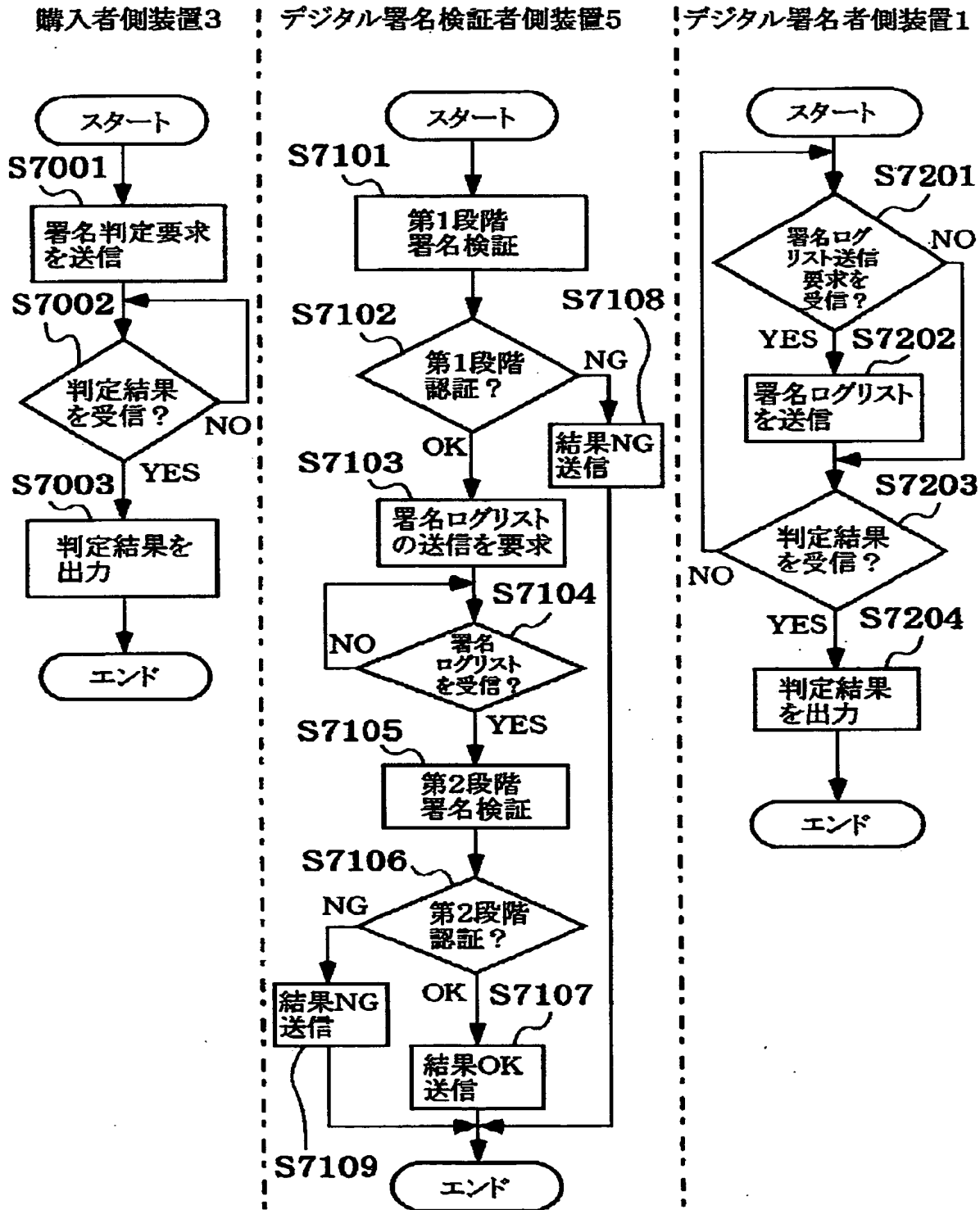


購入者側装置3



【図 5】

図 5



【図6】

図 6

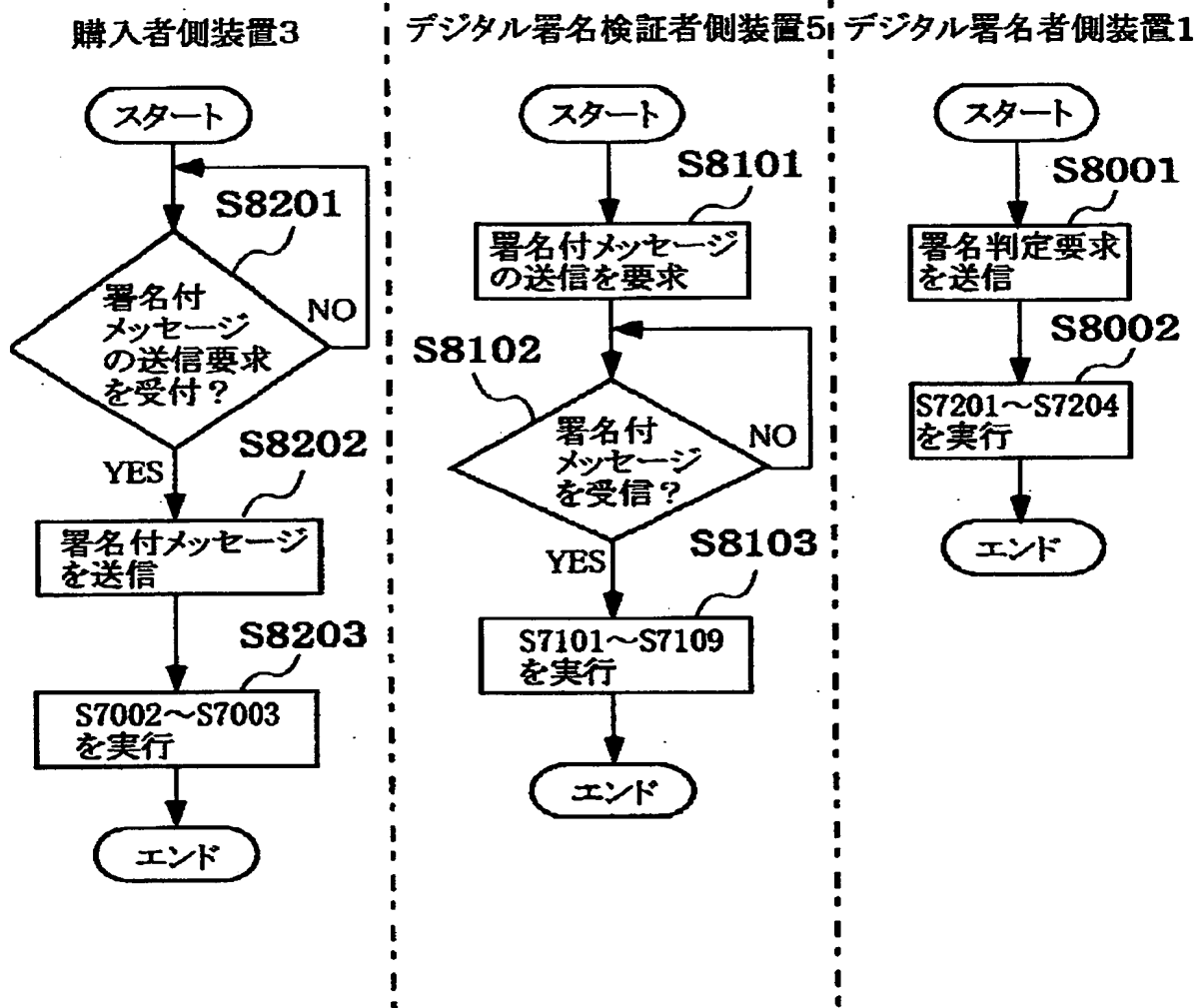
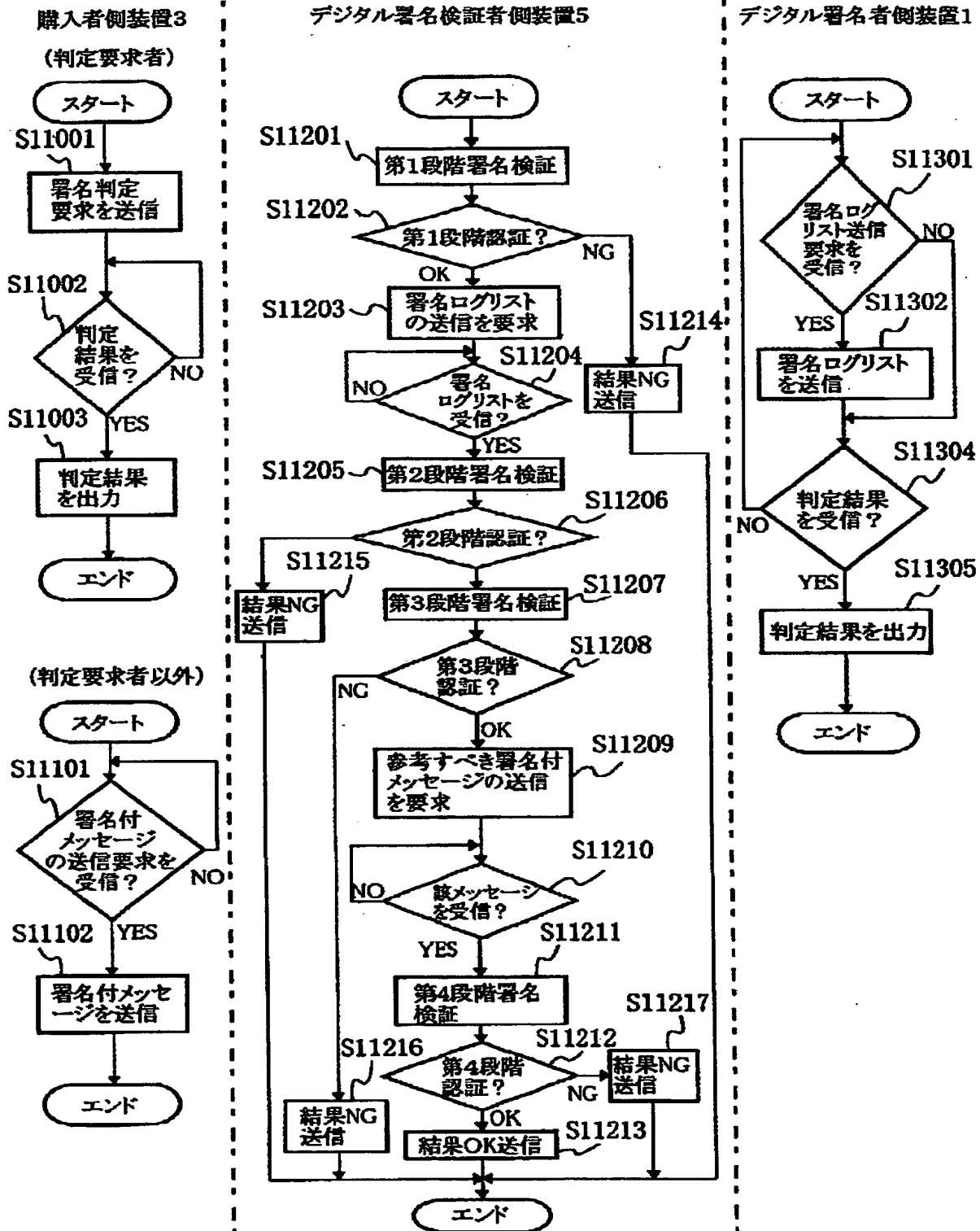


図 7
署名ログテーブル 2234
2235

前データ P_{N-1} ($h(M_{N-1}), \text{Sign}_{N-1}$)	メッセージ M_N の ハッシュ値 $h(M_N)$	(前データ P_{N-1} , メッセージ M_N) への署名 Sign_N	購入者名
前データ P_{N-2} ($h(M_{N-2}), \text{Sign}_{N-2}$)	メッセージ M_{N-1} の ハッシュ値 $h(M_{N-1})$	(前データ P_{N-2} , メッセージ M_{N-1}) への署名 Sign_{N-1}	購入者名
前データ P_1 ($h(M_1), \text{Sign}_1$)	メッセージ M_2 の ハッシュ値 $h(M_2)$	(前データ P_1 , メッセージ M_2) への署名 Sign_2	購入者名
初期値 IV	メッセージ M_1 の ハッシュ値 $h(M_1)$	(初期値 IV, メッセージ M_1) への署名 Sign_1	購入者名

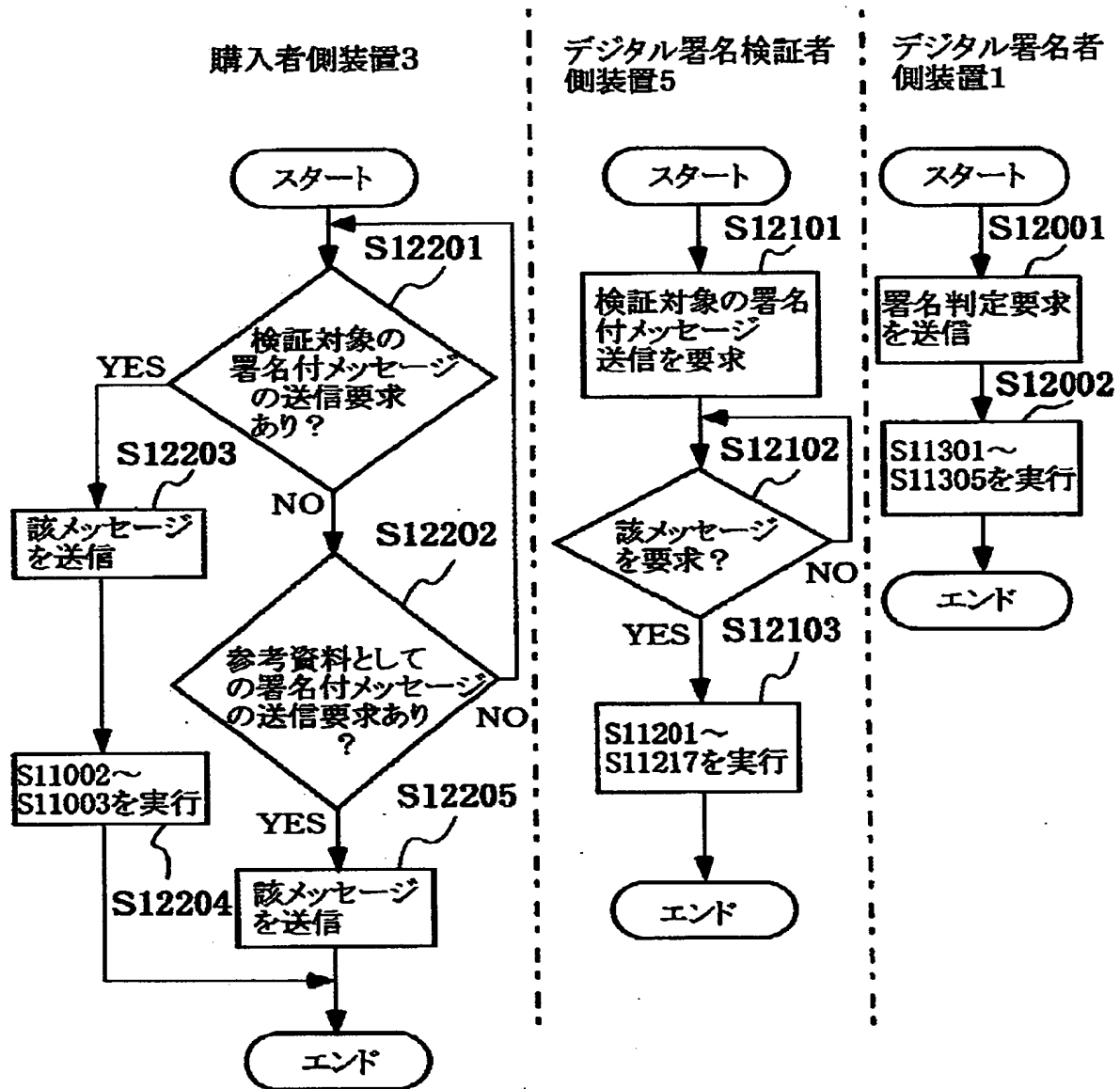
【図 8】

図 8



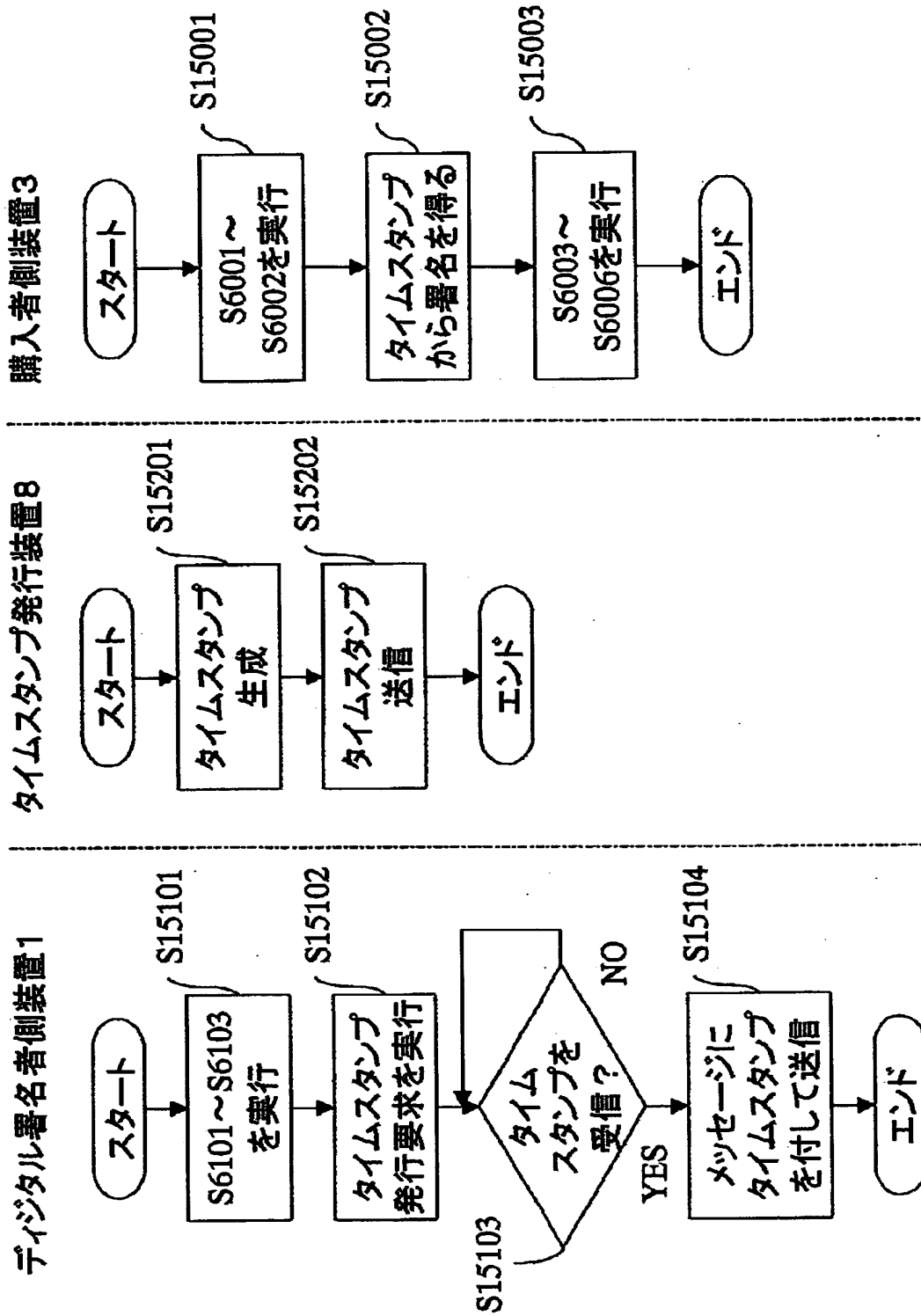
【図9】

図 9



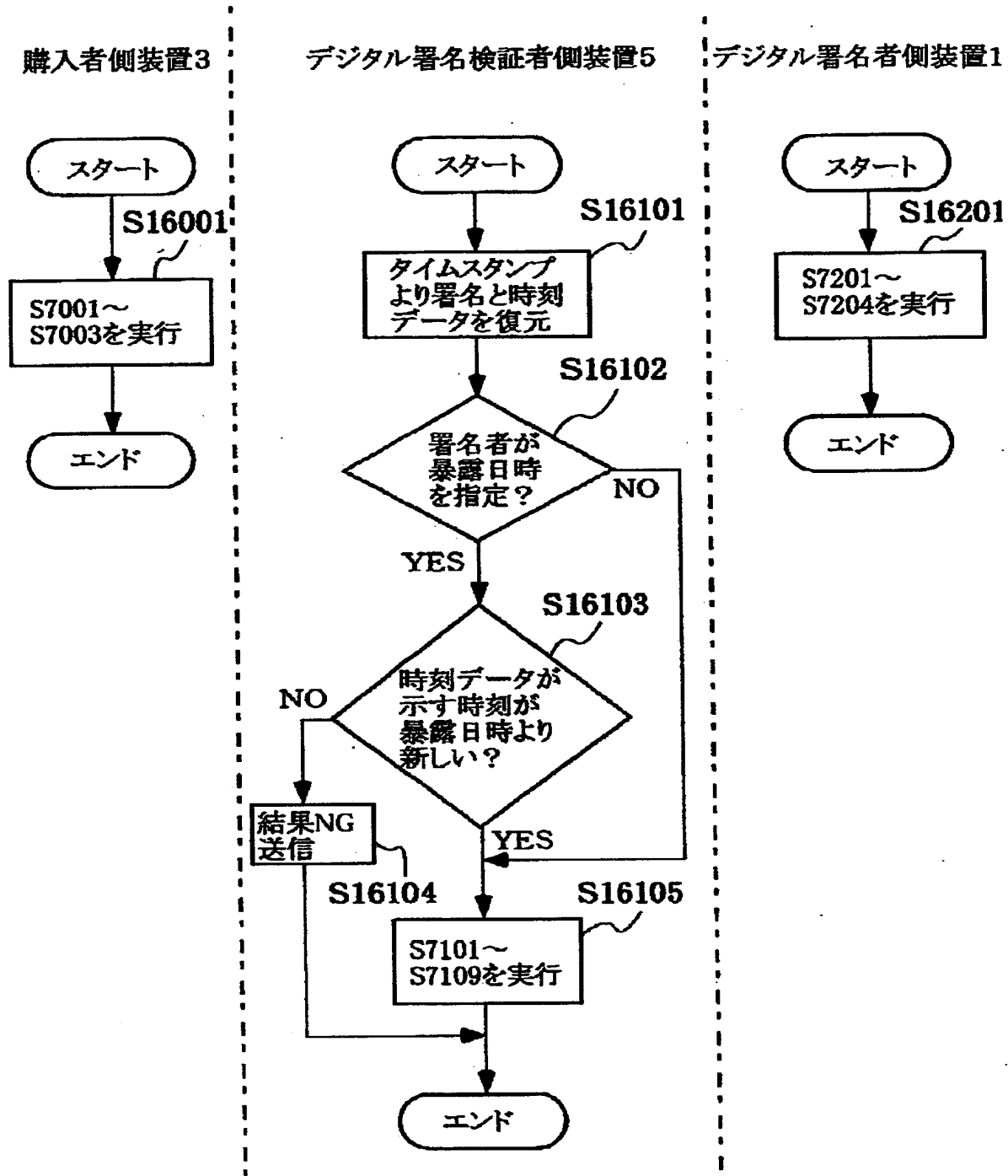
【図10】

図10



【図11】

図11



【図12】

図12

署名ログテーブル2234

2235

メッセージN のハッシュ値	メッセージN の署名	購入者名	タイムスタンプ
メッセージN-1 のハッシュ値	メッセージN-1 の署名	購入者名	なし
⋮			
メッセージN-m のハッシュ値	メッセージN-m の署名	購入者名	タイムスタンプ
メッセージN-m-1 のハッシュ値	メッセージN-m-1 の署名	購入者名	なし
⋮			
メッセージ2 のハッシュ値	メッセージ2 の署名	購入者名	なし
メッセージ1 のハッシュ値	メッセージ1 の署名	購入者名	タイムスタンプ

【書類名】 要約書

【要約】

【課題】

デジタル署名生成者自身がしたデジタル署名と第3者がデジタル署名生成者になりすまして行ったデジタル署名とを識別可能とする。

【解決手段】

デジタル署名者側装置1は、生成したデジタル署名とメッセージを含むデジタル署名付きメッセージの配布に先立ち、当該デジタル署名付きメッセージの署名ログ2235を署名ログテーブル2234に登録する。デジタル署名検証者側装置3は、デジタル署名者側装置1から署名ログリストを入手し、検証対象のデジタル署名付きメッセージが取得した署名ログリストに登録されているか否かを調べることで、当該デジタル署名付きメッセージがデジタル署名者側装置1で生成されたものであるか否かを検証する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号

[000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所